

# DATA RECORDER RESTORING ORIGINAL DATA ALLOWED TO EXIST ONLY UNIQUELY

**Publication number:** WO02075550 (A1)

**Publication date:** 2002-09-26

**Inventor(s):** HORI YOSHIHIRO [JP]

**Applicant(s):** SANYO ELECTRIC CO [JP]; HORI YOSHIHIRO [JP]

**Classification:**

- **international:** G06F21/00; G07F7/10; G06F21/00; G07F7/10; (IPC1-7): G06F12/14; G06F15/00; G06F17/60

- **European:** G06F21/00N1D1; G06F21/00N7D; G06F21/00N7T; G07F7/10D2P; G07F7/10D10M

**Application number:** WO2001JP07862 20010910

**Priority number(s):** JP20010073827 20010315

## Also published as:

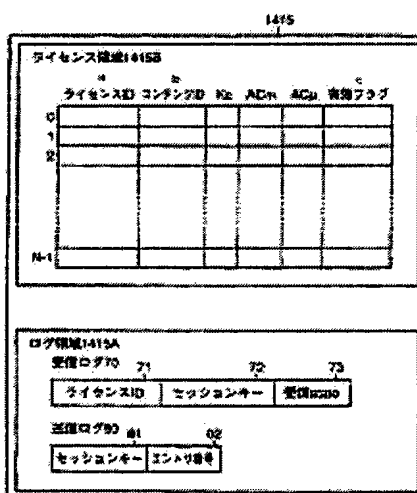
US2004088510 (A1)  
JP3696206 (B2)  
CN1493030 (A)  
CN1324484 (C)

## Cited documents:

JP2000305853 (A)  
JP2000285028 (A)  
JP2001051906 (A)  
JP2001014221 (A)  
JP2001022859 (A)

## Abstract of WO 02075550 (A1)

A log area (1415A) and a license area (1415B) are arranged in the memory of a memory card. In the license area (1415B), a license, e.g. a license ID and a license key Kc, and a validity flag, related to the entry number 0 to N-1 are stored. In the log area (1415A), a receiving log (70) and a transmission log (80) are stored. The transmission source of the license, i.e. the memory card, accepts a reception state from a destination memory card and validates the validity flag of an area designated by the entry number of the transmission log (80) if the reception state is on. Consequently, the license which is the object of transfer/duplicate can be restored even if the communication is interrupted during the transfer/duplicate of the license.



1415B...LICENSE AREA  
0...LICENSE ID  
1...SESSION KEY  
2...VALIDITY FLAG  
1415A...LOG AREA  
70...RECEPTION LOG  
71...LICENSE ID  
72...SESSION KEY  
73...RECEPTION STATE  
80...TRANSMISSION LOG  
81...SESSION KEY  
82...ENTRY NUMBER

Data supplied from the esp@cenet database — Worldwide

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2002 年 9 月 26 日 (26.09.2002)

PCT

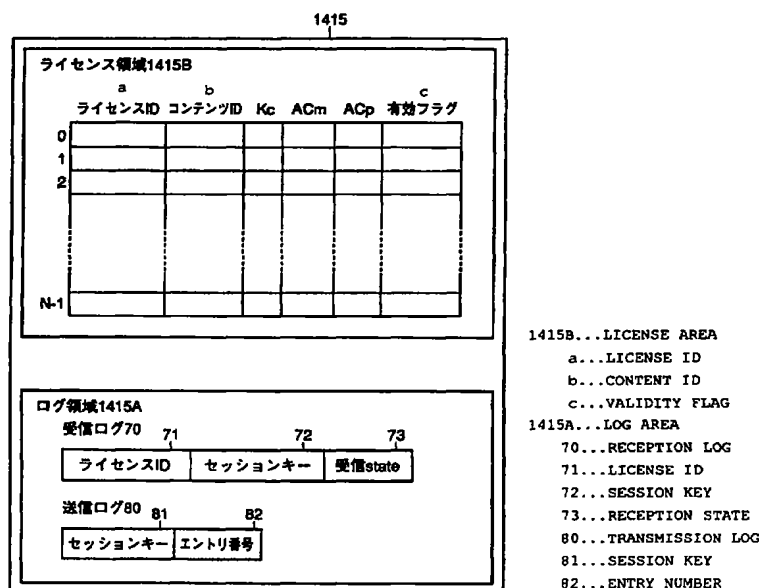
(10) 国際公開番号  
WO 02/075550 A1

- (51) 国際特許分類: G06F 12/14, 15/00, 17/60 (74) 代理人: 深見久郎, 外(FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 三井住友銀行南森町ビル Osaka (JP).
- (21) 国際出願番号: PCT/JP01/07862
- (22) 国際出願日: 2001 年 9 月 10 日 (10.09.2001) (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2001-73827 2001 年 3 月 15 日 (15.03.2001) JP
- (71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP).
- (72) 発明者; および (74) 発明者/出願人 (米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).
- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- 添付公開書類:  
— 国際調査報告書  
— 補正書

[続葉有]

(54) Title: DATA RECORDER RESTORING ORIGINAL DATA ALLOWED TO EXIST ONLY UNIQUELY

(54) 発明の名称: 一意義的にのみ存在が許容される独自データを復元可能なデータ記録装置



(57) Abstract: A log area (1415A) and a license area (1415B) are arranged in the memory of a memory card. In the license area (1415B), a license, e.g. a license ID and a license key Kc, and a validity flag, related to the entry number 0 to N-1 are stored. In the log area (1415A), a receiving log (70) and a transmission log (80) are stored. The transmission source of the license, i.e.

[続葉有]



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

the memory card, accepts a reception state from a destination memory card and validates the validity flag of an area designated by the entry number of the transmission log (80) if the reception state is on. Consequently, the license which is the object of transfer/duplicate can be restored even if the communication is interrupted during the transfer/duplicate of the license.

(57) 要約:

メモ리카ードのメモリにはログ領域(1415A)とライセンス領域(1415B)とが配置されている。そして、ライセンス領域(1415B)は、ライセンスIDおよびライセンス鍵Kc等のライセンスと有効フラグとをエントリ番号0~N-1に対応して格納する。ログ領域(1415A)は、受信ログ(70)と送信ログ(80)を含む。ライセンスの送信元であるメモ리카ードは、受信先のメモ리카ードから受信stateを受理し、受信stateがONであれば、送信ログ(80)のエントリ番号によって指定された領域の有効フラグを有効にする。その結果、ライセンスの移動/複製の途中で通信が切断されても、移動/複製の対象となったライセンスを復元できる。

## 明細書

一意義的にのみ存在が許容される独自データを復元可能なデータ記録装置

## 5 技術分野

この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンス等の一意義的にのみ存在が許容される独自データを他のデータ記録装置へ移動／複製するためのデータ記録装置に関するものである。

10

## 背景技術

近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

15

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

20

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

25

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽デ

ータを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、ライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツ

データとをメモ리카ードに送信する。そして、メモ리카ードは、受信したライセンス鍵と暗号化コンテンツデータとをメモ리카ードに記録する。

- 5       そして、メモ리카ードに記録した暗号化コンテンツデータを再生するときは、メモ리카ードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモ리카ードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

- 10       一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータの配信においては、パーソナルコンピュータにインストールされたソフトウェアによって暗号化コンテンツデータの配信が行なわれており、暗号化コンテンツデータに対するセキュリティは、暗号化コンテンツデータをメモ리카ードに書込む場合より低い。また、上記のメモ리카ードと同じセキュリティを持つデバイスをパーソナルコンピュータに装着すれば、上記の携帯電話機に対する暗号化コンテンツデータの配信と同じ配信をパーソナルコンピュータに対して行なうことが可能である。

- 20       そうすると、パーソナルコンピュータは、インストールされたソフトウェアと、上記デバイスとによって暗号化コンテンツデータを受信する。つまり、パーソナルコンピュータは、セキュリティレベルの異なる暗号化コンテンツデータを受信する。

- 25       さらに、音楽データが記録された音楽CDが広く普及しており、この音楽CDから音楽データをリッピングによって取得することも行なわれている。そして、このリッピングによって音楽データから暗号化音楽データ（暗号化コンテンツデータ）と、その暗号化音楽データを復号して再生するためのライセンスとが生成される。そして、このリッピングにおいては、コンテンツデータの利用規則を規定するウォーターマークをコンテンツデータから検出し、その検出したウォーターマークの内容に応じて暗号化コンテンツデータおよびライセンスが生成される。

上述したように、携帯電話機およびパーソナルコンピュータは、配信サーバから暗号化された暗号化コンテンツデータおよびライセンスを受信する。そして、携帯電話機およびパーソナルコンピュータのユーザは、受信した暗号化コンテンツデータおよびライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ移動または複製することもある。この場合、ユーザは、暗号化コンテンツデータを他のユーザの携帯電話機またはパーソナルコンピュータへ移動／複製することは自由であるが、暗号化コンテンツデータを復号するライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ自由に移動することはできない。つまり、ライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ移動／複製したとき、暗号化コンテンツデータの著作権保護の観点から送信側と受信側との両方にライセンスを残すことはできない。そこで、ライセンスの移動／複製を行なったとき、送信側のライセンスを消去する。

しかし、従来のライセンスの移動／複製の方法では、他のユーザへのライセンスの移動／複製の途中で通信が切断されたとき、他のユーザへはライセンスが届かず、送信側でもライセンスが消去された状態となり、移動／複製の対象となったライセンスを用いて暗号化コンテンツデータを復号できないという問題が生じる。

#### 発明の開示

それゆえに、この発明の目的は、ライセンス等の一意的にのみ存在が許容される独自データを他のデータ記録装置へ移動する途中で通信が切断されたときも、移動の対象となった独自データを復元可能なデータ記録装置を提供することである。

この発明によれば、データ記録装置は、一義的にのみ存在することが許容される独自データを他のデータ記録装置へ移動するデータ記録装置であって、他のデータ記録装置への独自データの移動処理を特定するための第1の履歴情報を保持する履歴情報保持部と、独自データを保持する独自データ保持部と、制御部とを備え、制御部は、独自データの他のデータ記録装置への移動に対して独自データの外部への出力が不可能な状態に変更し、独自データの復元要求に応じて、他の

データ記録装置との通信状態を示す他のデータ記録装置に保持された通信情報と他のデータ記録装置に保持された移動処理を特定するための第2の履歴情報とを他のデータ記録装置から受信し、通信情報に基づいて他のデータ記録装置との通信状態を確認し、通信情報が移動の途中を示すとき第2の履歴情報が第1の履歴情報に一致するか否かを判定し、第2の履歴情報が第1の履歴情報に一致するとき独自データの外部への出力が可能な状態に復元する。

好ましくは、独自データ保持部は、独自データの一部または全てを外部へ出力可能か出力不可かを示す出力可否フラグをさらに保持し、制御部は、独自データの他のデータ記録装置への移動に対して出力可否フラグを出力不可に設定し、独自データの復元時、出力可否フラグを出力可能に設定する。

好ましくは、履歴情報保持部は、移動の対象となった独自データを外部へ出力不可能な状態でさらに保持し、制御部は、独自データの他のデータ記録装置への移動に対して移動の対象となった独自データを履歴情報保持部に与え、独自データ保持部から移動の対象となった独自データを消去し、独自データの復元時、履歴情報保持部に保持された独自データを独自データ保持部に書込む。

好ましくは、第1の履歴情報は、移動のための通信確立時に他のデータ記録装置で生成され、かつ、他のデータ記録装置から受信された第1のセッション鍵であり、第2の履歴情報は、移動のための通信確立時に他のデータ記録装置で生成され、かつ、他のデータ記録装置に保持された第1のセッション鍵と同じ第2のセッション鍵である。

好ましくは、電子署名により通信情報と第2の履歴情報との正当性を確認する署名確認手段をさらに備え、制御部は、さらに、通信情報と第2の履歴情報とに対する電子署名を通信情報および第2の履歴情報とともに他のデータ記録装置から受信し、署名確認手段によって通信情報と第2の履歴情報の正当性が確認されたとき、通信状態を確認し、かつ、第1の履歴情報と第2の履歴情報との一致を確認する。

好ましくは、他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部と、セッション鍵生成部が生成したセッション鍵によって暗号化されたデータを復号する復号部とをさらに備え、独自データの復元



時、セッション鍵生成部は、独自データの復元のための通信を特定する第3のセッション鍵を生成し、制御部は、第3のセッション鍵を他のデータ記録装置へ送信し、第3のセッション鍵によって暗号化された第2の履歴情報を他のデータ記録装置から受信する。

- 5       好ましくは、他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部と、セッション鍵生成部が生成したセッション鍵によって暗号化されたデータを復号する復号部とをさらに備え、独自データの復元時、セッション鍵生成部は、独自データの復元のための通信を特定する第3のセッション鍵を生成し、制御部は、第3のセッション鍵を他のデータ記録装置へ送信し、第3のセッション鍵によって暗号化された第2の履歴情報と、第3のセッション鍵によって暗号化された電子署名のデータとを他のデータ記録装置から受信する。

- 15       好ましくは、履歴情報保持部は、移動の対象となった独自データに含まれる第1のデータ特定情報を第1の履歴情報とともに保持し、制御部は、さらに、他のデータ記録装置から受信する移動の対象となった第2のデータ特定情報が第1のデータ特定情報に一致するか否かを判定し、第2のデータ特定情報が第1のデータ特定情報に一致するとき、通信情報を確認し、かつ、第1の履歴情報と第2の履歴情報との一致を確認する。

- 20       好ましくは、電子署名により通信情報と第2の履歴情報と第2のデータ特定情報との正当性を確認する署名確認手段をさらに備え、制御部は、さらに、通信情報と第2の履歴情報と第2のデータ特定情報とに対する電子署名を、通信情報と第2の履歴情報と第2のデータ特定情報とともに受信し、署名確認手段によって通信情報と第2の履歴情報と第2のデータ特定情報の正当性が確認されたとき、第2のデータ特定情報と第1のデータ特定情報との一致を確認し、かつ、通信情報を確認し、第1の履歴情報と第2の履歴情報との一致を確認する。

- 25       好ましくは、他のデータ記録装置または他のデータ記録装置と異なるもう1つの他のデータ記録装置との通信状態を示すもう1つの通信情報を保持する通信情報保持部と、他のデータ記録装置またはもう1つの他のデータ記録装置からの独自データの移動処理を特定するための第3の履歴情報を保持するもう1つの履歴

情報保持部とをさらに備え、制御部は、独自データの移動処理において移動対象となる独自データを他のデータ記録装置またはもう 1 つの他のデータ記録装置から受信するとき、第 3 の履歴情報をもう 1 つの履歴情報保持部に記録し、外部からの履歴情報の出力要求に応じて通信情報と第 3 の履歴情報とを出力する。

- 5       好ましくは、他のデータ記録装置またはもう 1 つの他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部をさらに備え、セッション鍵生成部は、独自データの移動処理において移動対象となる独自データを他のデータ記録装置またはもう 1 つの他のデータ記録装置から受信するための通信を特定する第 4 のセッション鍵を生成し、制御部は、移動対象となる独自
- 10       データを他のデータ記録装置またはもう 1 つのデータ記録装置から受信する通信の確立時、第 4 のセッション鍵を他のデータ記録装置またはもう 1 つのデータ記録装置へ送信するとともに第 4 のセッション鍵を第 3 の履歴情報としてもう 1 つの履歴情報保持部に格納し、外部からの履歴情報の出力要求に応じてもう 1 つの通信情報および第 3 の履歴情報を出力する。

- 15       好ましくは、もう 1 つの通信情報と第 3 の履歴情報とに対する電子署名を生成する電子署名生成部をさらに備え、制御部は、外部からの履歴情報の出力要求に応じて、もう 1 つの通信情報と第 3 の履歴情報と電子署名とを出力する。

- 好ましくは、他のデータ記録装置またはもう 1 つの他のデータ記録装置から入力された第 5 のセッション鍵によって暗号化する暗号処理部をさらに備え、制御
- 20       部は、他のデータ記録装置またはもう 1 つの他のデータ記録装置から独自データを受信する通信の確立時、第 4 のセッション鍵を他のデータ記録装置またはもう 1 つの他のデータ記録装置に出力するとともに第 4 のセッション鍵を第 3 の履歴情報としてもう 1 つの履歴情報保持部に格納し、外部からの履歴情報の出力要求に応じてもう 1 つの通信情報と暗号処理部において第 5 のセッション鍵によって
- 25       暗号化された第 3 の履歴情報とを出力する。

好ましくは、他のデータ記録装置またはもう 1 つの他のデータ記録装置から入力された第 5 のセッション鍵によってデータを暗号化する暗号処理部と、通信情報と暗号処理部において外部から入力された第 3 のセッション鍵によって暗号化された第 3 の履歴情報とに対する電子署名を生成する電子署名生成部とをさらに

備え、暗号処理部は、第 5 のセッション鍵によって第 3 の履歴情報と電子署名とを暗号化し、制御部は、他のデータ記録装置またはもう 1 つの他のデータ記録装置から独自データを受信する通信の確立時、第 4 のセッション鍵を他のデータ記録装置またはもう 1 つの他のデータ記録装置に出力するとともに第 4 のセッション鍵を第 3 の履歴情報としてもう 1 つの履歴情報保持部に格納し、外部からの履歴情報の出力要求に応じて、通信情報と第 5 のセッション鍵によって暗号化された第 3 の履歴情報と第 5 のセッション鍵によって暗号化された電子署名とを出力する。

好ましくは、制御部は、他のデータ記録装置またはもう 1 つの他のデータ記録装置からの移動の対象となる独自データを特定する第 3 のデータ特定情報を通信情報保持部に記録し、第 3 のデータ特定情報の出力要求に応じて、通信情報保持部から第 3 のデータ特定情報を読み出して通信情報および第 3 の履歴情報とともに出力する。

好ましくは、独自データは、暗号化コンテンツデータを復号するためのライセンスである。

したがって、この発明によれば、他のデータ記録装置へ一義的にのみ存在することが許容される独自データを移動させている途中で通信が切断されても、移動の対象となった独自データを復元することができる。

## 20 図面の簡単な説明

図 1 は、データ配信システムを概念的に説明する概略図である。

図 2 は、他のデータ配信システムを概念的に説明する概略図である。

図 3 は、図 1 および図 2 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

25 図 4 は、図 1 および図 2 に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

図 5 は、図 1 および図 2 に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

図 6 は、図 1 および図 2 に示すデータ配信システムにおけるパーソナルコンピ

ュータの構成を示す概略ブロック図である。

図 7 は、図 2 に示すデータ配信システムにおける再生端末の構成を示す概略ブロック図である。

5 図 8 は、図 1 および図 2 に示すデータ配信システムにおけるメモ리카ードの構成を示す概略ブロック図である。

図 9 は、図 1 および図 2 に示すデータ配信システムにおける配信動作を説明するための第 1 のフローチャートである。

図 10 は、図 1 および図 2 に示すデータ配信システムにおける配信動作を説明するための第 2 のフローチャートである。

10 図 11 は、パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

図 12 は、メモ리카ードにおける再生リストファイルの構成を示す図である。

図 13 は、メモ리카ード間の移動動作の概念を説明するための概略ブロック図である。

15 図 14 は、図 1 および図 2 に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動／複製動作を説明するための第 1 のフローチャートである。

20 図 15 は、図 1 および図 2 に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動／複製動作を説明するための第 2 のフローチャートである。

図 16 は、図 1 および図 2 に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動／複製動作を説明するための第 3 のフローチャートである。

図 17 は、メモ리카ードのログ領域を説明するための概略ブロック図である。

25 図 18 は、ライセンスの復元動作を説明するための第 1 のフローチャートである。

図 19 は、ライセンスの復元動作を説明するための第 2 のフローチャートである。

図 20 は、携帯電話機または再生端末における再生動作を説明するためのフロ

ーチャートである。

#### 発明を実施するための最良の形態

5 本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

図1は、本発明によるデータ記録装置が暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

10 なお、以下では携帯電話網を介して音楽データをユーザの携帯電話機に装着されたメモリカード110に、またはインターネットを介して音楽データを各パーソナルコンピュータに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画画像データ等を配信する場合においても適用することが可能なものである。

15 図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行なう。  
20 そして、配信サーバ10は、正当なメモリカードに対して著作権を保護するために所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含む  
25 むライセンスを与える。

配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能

なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、著作権を保護するために行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生回路（図示せず）に与える。

- 5      さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

- 10      このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ10からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

- 15      しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

- 20      また、図1においては、配信サーバ10は、インターネット網30を通じて得た、パーソナルコンピュータ50のユーザからの配信要求を受信する。そうすると、配信サーバ10は、データ配信を求めてアクセスして来たパーソナルコンピュータ50が正当な認証データを持つライセンス専用メモリカード（図示せず）を利用してアクセスしているか否か、すなわち、正規のライセンス専用メモリカードであるか否かの認証処理を行なう。そして、配信サーバ10は、正当なライセンス専用メモリカードを備えたパーソナルコンピュータに対して、著作権を保護するために所定の暗号方式により音楽データを暗号化した暗号化コンテンツデータおよびその復号鍵であるライセンス鍵を含むライセンスをインターネット網  
25      30を介して送信する。パーソナルコンピュータ50のライセンス専用メモリカードはライセンスを格納する。

パーソナルコンピュータ50は、メモリカード110のライセンス管理に関わる機能と同一機能を備えたライセンス専用メモリカード（ハードウェア）を備えることで、携帯電話機100およびメモリカード110を用いて受信したのと同

じ配信を受けることができる。

さらに、パーソナルコンピュータ 50 は、専用ケーブル 65 によって携帯電話機 100 と接続され、暗号化コンテンツデータおよびライセンスを携帯電話機 100 に装着されたメモリカード 110 へ送信することが可能である。

5       したがって、図 1 に示すデータ配信システムにおいては、携帯電話機 100 に装着されたメモリカード 110 は、携帯電話網を介して配信サーバ 10 から暗号化コンテンツデータおよびライセンスを受信して格納するとともに、パーソナルコンピュータ 50 がインターネット網 30 を介して配信サーバ 10 から取得した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ 50 から受  
10       けて格納することができる。

さらに、携帯電話機 100 に装着されたメモリカード 110 は、携帯電話網を介して配信サーバ 10 から受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ 50 に待避することが可能となる。

図 2 は、携帯電話網を介して配信サーバ 10 から暗号化コンテンツデータおよび  
15       ライセンスを受信する機能を有しない再生端末 102 を用いた場合のデータ配信システムを示したものである。図 2 に示すデータ配信システムにおいては、再生端末 102 に装着されたメモリカード 110 は、パーソナルコンピュータ 50 が配信サーバ 10 から取得した暗号化コンテンツデータおよびライセンスを受け  
20       て格納する。このように、パーソナルコンピュータ 50 が暗号化コンテンツデータおよびライセンスを取得することによって通信機能のない再生端末 102 のユーザも暗号化コンテンツデータを受信することができるようになる。

図 1 および図 2 に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機またはパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第 1 には、通信におけるライセンスを  
25       配信するための方式であり、さらに第 2 には、コンテンツデータを暗号化する方式そのものであり、さらに、第 3 には、このようなコンテンツデータの無断コピーを防止するための著作権保護を実現する構成である。

本発明の実施の形態においては、特に、配信、および再生の各処理の発生時において、これらのライセンス鍵の出力先に対する認証およびチェック機能を充実

させ、非認証の記録装置（メモリカードおよびライセンス専用メモリカードなど）および再生端末（コンテンツ再生回路を備える携帯電話機やパーソナルコンピュータなど）に対するコンテンツデータの出力を防止することによってライセンス鍵の流出を防ぎ、著作権の保護を強化する構成を説明する。

- 5       なお、以下の説明においては、配信サーバ10から、各携帯電話機、各パーソナルコンピュータ等に暗号化コンテンツデータまたはそのライセンスを伝送する処理を「配信」と称することとする。

図3は、図1および図2に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

- 10       まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ {Dc} Kcがこの形式で配信サーバ10より携帯電話機100またはパーソナルコンピュータ50のユーザに配布される。

- 15       なお、以下においては、{Y} Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

- さらに、配信サーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc-infが配布される。また、ライセンスとしては、ライセンス鍵Kc、  
20       c、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp等が存在する。ライセンスIDは、配信サーバ10からのライセンスの配信を管理し、ライセンスを識別するためのコードであり、コンテンツIDは、コンテンツデータDcおよびライセンス鍵Kcを識別するためのコードである。アクセス制御情報ACmは、記録装置（メモリカード、またはライセンス専用メモリカード）におけるライセンスのアクセスに対する制限に関する情報である。  
25       また、再生制御情報ACpは、コンテンツ再生回路における再生に関する制御情報である。具体的には、アクセス制御情報ACmは、メモリカード、およびライセンス専用メモリカードからのライセンスまたはライセンス鍵を外部に出力するに当たっての制御情報であり、再生可能回数（再生のためにライセンス鍵を出



力する数)、ライセンスの移動・複製に関する制限情報などがある。再生制御情報ACpは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、および再生範囲指定(部分ライセンス)などがある。

- 5       以後、ライセンスIDと、コンテンツIDと、ライセンス鍵Kcと、アクセス制御情報ACmと、再生制御情報ACpとを併せて、ライセンスと総称することとする。

- また、以降では、簡単化のためアクセス制御情報ACmは再生回数の制限を行なう制御情報である再生回数(0:再生不可、1~254:再生可能回数、255:制限無し)、ライセンスの移動および複製を制限する移動・複製フラグ(0:移動複製禁止、1:移動のみ可、2:移動複製可)の2項目とし、再生制御情報ACpは再生可能な期限を規定する制御情報である再生期限(UTCtimeコード)のみを制限するものとする。
- 10

- 本発明の実施の形態においては、送信元の記録装置(メモリカード、またはライセンス専用メモリカード)から受信先の記録装置へのライセンスの移動/複製において、送信元の記録装置に保持されたライセンスの有効・無効を示す有効フラグの運用を行なう。この有効フラグが有効であるとき、ライセンスをメモリカードから外部へ出すことが可能であることを意味し、有効フラグが無効であるとき、ライセンスをメモリカードから外部へ出すことができないことを意味する。
- 15

- 図4は、図1および図2に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。
- 20

- データ再生端末内のコンテンツ再生回路、メモリカード、およびライセンス専用メモリカードには固有の公開暗号鍵KPyおよびKpmwがそれぞれ設けられる。公開暗号鍵KPyは、コンテンツ再生回路に固有の秘密復号鍵Kpyによって復号可能である。また、公開暗号鍵Kpmwは、メモリカード、およびライセンス専用メモリカードに固有の秘密復号鍵Kmwによって復号可能である。これら公開暗号鍵および秘密復号鍵は、メモリカード、およびライセンス専用メモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号
- 25

鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

また、コンテンツ再生回路のクラス証明書としてC p yが設けられ、メモリカード、およびライセンス専用メモリカードのクラス証明書としてC m wが設けられる。これらのクラス証明書は、コンテンツ再生回路、メモリカード、およびライセンス専用メモリカードのクラスごとに異なる情報を有する。

コンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ {K P p y / / C p y} K P a の形式で出荷時にデータ再生回路に記録される。また、メモリカード、およびライセンス専用メモリカードのクラス公開暗号鍵およびクラス証明書は認証データ {K P m w / / C m w} K P a の形式で出荷時にメモリカード、およびライセンス専用メモリカードにそれぞれ記録される。後ほど詳細に説明するが、K P a は配信システム全体で共通の公開認証鍵である。

また、メモリカード110、およびライセンス専用メモリカード内のデータ処理を管理するための鍵として、メモリカード110、およびライセンス専用メモリカードという媒体ごとに設定される公開暗号鍵K P m c x と、公開暗号鍵K P m c x で暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵K m c x が存在する。これらのメモリカードおよびライセンス専用メモリカードごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵K P m c x を個別公開暗号鍵、秘密復号鍵K m c x を個別秘密復号鍵と称する。

ライセンスの配信、移動、複製および再生が行なわれるごとに配信サーバ10、携帯電話機100、メモリカード110、およびライセンス専用メモリカードにおいて生成される共通鍵K s 1 ~ K s 3 が用いられる。

ここで、共通鍵K s 1 ~ K s 3 は、配信サーバ、コンテンツ再生回路もしくはメモリカードもしくはライセンス専用メモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵K s 1 ~ K s 3 を「セッションキー」とも呼ぶこととする。

これらのセッションキーK s 1 ~ K s 3 は、各セッションごとに固有の値を有

することにより、配信サーバ、コンテンツ再生回路、メモリカード、およびライセンス専用メモリカードによって管理される。具体的には、セッションキーK s 1は、配信サーバによって配信セッションごとに発生される。セッションキーK s 2は、メモリカード、およびライセンス専用メモリカードによって配信セッションおよび再生セッションごとに発生され、セッションキーK s 3は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

図5は、図1および図2に示した配信サーバ10の構成を示す概略ブロック図である。

配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツID等の配信情報を保持するための情報データベース304と、携帯電話機やパーソナルコンピュータの各ユーザごとにコンテンツデータへのアクセスの開始に従った課金情報を保持するための課金データベース302と、情報データベース304に保持されたコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315によって制御され、配信セッション時にセッションキーK s 1を発生するためのセッションキー発生部316と、メモリカード、およびライセンス専用メモリカードから送られてきた認証のための認証データ {K P m w / / C m w} K P a を復号するための

公開認証鍵K P aを保持する認証鍵保持部3 1 3と、メモリカード、およびライセンス専用メモリカードから送られてきた認証のための認証データ {K P m w / C m w} K P aを通信装置3 5 0およびバスB S 1を介して受けて、認証鍵保持部3 1 3からの公開認証鍵K P aによって復号処理を行なう復号処理部3 1 2  
5 と、配信セッションごとに、セッション鍵K s 1を発生するセッションキー発生部3 1 6、セッションキー発生部3 1 6より生成されたセッションキーK s 1を復号処理部3 1 2によって得られたクラス公開暗号鍵K P m wを用いて暗号化して、バスB S 1に出力するための暗号処理部3 1 8と、セッションキーK s 1によって暗号化された上で送信されたデータをバスB S 1より受けて、セッション  
10 キーK s 1により復号処理を行なう復号処理部3 2 0とを含む。

データ処理部3 1 0は、さらに、配信制御部3 1 5から与えられるライセンス鍵K cおよびアクセス制御情報A C mを、復号処理部3 2 0によって得られたメモリカード、およびライセンス専用メモリカードごとに個別な公開暗号鍵K P m c xによって暗号化するための暗号処理部3 2 6と、暗号処理部3 2 6の出力  
15 を、復号処理部3 2 0から与えられるセッションキーK s 2によってさらに暗号化してバスB S 1に出力するための暗号処理部3 2 8とを含む。

配信サーバ1 0の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図6は、図1および図2に示したパーソナルコンピュータ5 0の構成を説明するための概略ブロック図である。パーソナルコンピュータ5 0は、パーソナルコンピュータ5 0の各部のデータ授受を行なうためのバスB S 2と、パーソナルコンピュータ5 0内を制御すると共に、各種のプログラムを実行するためのコントローラ(C P U) 5 1 0と、バスB S 2に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク(HDD) 5 3 0  
20 およびC D-R O Mドライブ5 4 0と、ユーザからの指示を入力するためのキーボード5 6 0と、各種の情報を視覚的にユーザに与えるためのディスプレイ5 7 0とを含む。

パーソナルコンピュータ5 0は、さらに、暗号化コンテンツデータおよびライセンスを携帯電話機1 0 0等へ通信する際にコントローラ5 1 0と端子5 8 0と

の間でデータの授受を制御するためのUSB (Universal Serial Bus) インタフェース550と、専用ケーブル65またはUSBケーブル75を接続するための端子580と、インターネット網30を介して配信サーバ10と通信する際にコントローラ510と端子585との間でデータの授受を制御するためのモデム555と、インターネット網30と接続するための端子585とを含む。

コントローラ510は、インターネット網30を介してライセンス専用メモリカード520に暗号化コンテンツデータ等を配信サーバ10から受信するために、配信サーバ10との間でデータの授受を制御する。さらに、パーソナルコンピュータ50は、配信サーバ10からの暗号化コンテンツデータおよびライセンスの受信を行なう際に配信サーバ10との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス専用メモリカード520と、バスBS2とライセンス専用メモリカード520との間でデータの授受を行なうメモリカードインタフェース525とを含む。

ライセンス専用メモリカード520は、暗号化コンテンツデータおよびライセンスを配信サーバ10から受信する際のデータの授受をハード的に行ない、受信したライセンスをハード的に管理する。

このように、パーソナルコンピュータ50は、配信サーバ10からインターネット網30を介して暗号化コンテンツデータおよびライセンスを受信したり、メモリカード110から待避されたライセンスを格納するためのライセンス専用メモリカード520を内蔵するものである。

図7は、図2に示した再生端末102の構成を説明するための概略ブロック図である。

再生端末102は、再生端末102の各部のデータ授受を行なうためのバスBS3と、バスBS3を介して再生端末102の動作を制御するためのコントローラ1106と、外部からの指示を再生端末102に与えるための操作パネル1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるための表示パネル1110とを含む。

再生端末102は、さらに、配信サーバ10からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード110と、メモリカード110とバスBS3との間のデータの授受を制御するためのメモリカードインタフェース1200と、パーソナルコンピュータ50から暗号化  
5 コンテンツデータおよびライセンスを受信する際にバスBS3と端子1114との間のデータ授受を制御するためのUSBインタフェース1112と、USBケーブル75を接続するための端子1114とを含む。

再生端末102は、さらに、クラス公開暗号鍵K<sub>Pp</sub>1およびクラス証明書C<sub>p</sub>1を公開認証鍵K<sub>Pa</sub>で復号することでその正当性を認証できる状態に暗号化した認証データ {K<sub>Pp</sub>1//C<sub>p</sub>1} K<sub>Pa</sub>を保持する認証データ保持部15  
10 00を含む。ここで、再生端末102のクラス $y$ は、 $y=1$ であるとする。

再生端末102は、さらに、クラス固有の復号鍵であるK<sub>p</sub>1を保持するK<sub>p</sub>保持部1502と、バスBS3から受けたデータを復号鍵K<sub>p</sub>1によって復号し、メモリカード110によって発生されたセッションキーK<sub>s</sub>2を得る復号処  
15 理部1504とを含む。

再生端末102は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS3上においてやり取りされるデータを暗号化するためのセッションキーK<sub>s</sub>3を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵K<sub>c</sub>および再生制御情報AC<sub>p</sub>を受取る際に、セッションキー発生部1508により発生され  
20 たセッションキーK<sub>s</sub>3を復号処理部1504によって得られたセッションキーK<sub>s</sub>2によって暗号化し、バスBS3に出力する暗号処理部1506とを含む。

再生端末102は、さらに、バスBS3上のデータをセッションキーK<sub>s</sub>3によって復号して、ライセンス鍵K<sub>c</sub>および再生制御情報AC<sub>p</sub>を出力する復号処理部1510と、バスBS3より暗号化コンテンツデータ {D<sub>c</sub>} K<sub>c</sub>を受け  
25 て、復号処理部1510からのライセンス鍵K<sub>c</sub>によって暗号化コンテンツデータ {D<sub>c</sub>} K<sub>c</sub>を復号してコンテンツデータD<sub>c</sub>を音楽再生部1518へ出力する復号処理部1516とを含む。

再生端末102は、さらに、復号処理部1516からの出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518の出力をデジタル信号からアナログ信号に変換するDA変換器1519と、DA変換器1519の出力をヘッドホンなどの外部出力装置（図示省略）へ出力するための端子1530とを含む。

なお、図7においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生回路1550を構成する。

一方、図1に示す携帯電話機100は、携帯電話網を介して配信サーバ10から暗号化コンテンツデータあるいはライセンスの配信を受信する機能を有するものである。したがって、図1に示す携帯電話機100の構成は、図7に示す構成において、携帯電話網により無線伝送される信号を受信するためのアンテナと、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナに与えるための送受信部とマイクとスピーカと音声コーデック等の携帯電話機が本来備える機能を設けたものである。また、USBインタフェース1112と端子1114とに代えて、それぞれ、専用ケーブルを接続するための専用インタフェースと専用端子とを備える。

携帯電話機100、および再生端末102の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図8は、図1および図2に示すメモリカード110の構成を説明するための概略ブロック図である。

既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、 $KPmw$ および $Kmw$ が設けられ、メモリカードのクラス証明書 $Cmw$ が設けられるが、メモリカード110においては、自然数 $w=3$ で表わされるものとする。また、メモリカードを識別する自然数 $x$ は $x=4$ で表されるものとする。

したがって、メモリカード110は、認証データ $\{KPm3//Cm3\}$   $KPa$ を保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵 $Kmc4$ を保持する $Kmc$ 保持部1402と、クラス秘密復号鍵 $Km3$ を保持する $Km$ 保持部1421と、個別秘密復号鍵 $Kmc$

4によって復号可能な公開暗号鍵 $K_{Pmc4}$ を保持する $K_{Pmc}$ 保持部1416を含む。

このように、メモ리카ードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモ리카ード単位で実行することが可能になる。

メモ리카ード110は、さらに、メモ리카ードインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS4と、バスBS4にインタフェース1424から与えられるデータを、 $K_m$ 保持部1421からのクラス秘密復号鍵 $K_{m3}$ により復号して、配信サーバ10が配信セッションにおいて生成したセッションキー $K_{s1}$ を接点Paに出力する復号処理部1422と、 $K_{Pa}$ 保持部1414から公開認証鍵 $K_{Pa}$ を受けて、バスBS4に与えられるデータから公開認証鍵 $K_{Pa}$ による復号処理を実行して復号結果と得られたクラス証明書をコントローラ1420に、得られたクラス公開鍵を暗号処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS4に出力する暗号処理部1406を含む。

メモ리카ード110は、さらに、配信、および再生の各セッションにおいてセッションキー $K_{s2}$ を発生するセッションキー発生部1418と、セッションキー発生部1418が出力したセッションキー $K_{s2}$ を復号処理部1408によって得られるクラス公開暗号鍵 $K_{Ppy}$ もしくは $K_{Pmw}$ によって暗号化してバスBS4に送出する暗号処理部1410と、バスBS4よりセッションキー $K_{s2}$ によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキー $K_{s2}$ によって復号する復号処理部1412と、暗号化コンテンツデータの再生セッションにおいてメモリ1415から読出されたライセンス鍵 $K_c$ および再生制御情報 $ACp$ を、復号処理部1412で復号された他のメモ리카ードの個別公開暗号鍵 $K_{Pmcx}$  ( $x \neq 4$ )で暗号化する暗号処理部1417とを含む。

メモ리카ード110は、さらに、バスBS4上のデータを個別公開暗号鍵 $K_P$



m c 4 と対をなすメモリカード 1 1 0 の個別秘密復号鍵 K m c 4 によって復号するための復号処理部 1 4 0 4 と、配信サーバ 1 0 や他のメモリカードとの間の通信における履歴を格納するログと、暗号化コンテンツデータ {D c} K c と、暗号化コンテンツデータ {D c} K c を再生するためのライセンス (K c, A C p, A C m, ライセンス I D, コンテンツ I D) と、付加情報 D c - i n f と、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバス B S 4 より受けて格納するためのメモリ 1 4 1 5 とを含む。メモリ 1 4 1 5 は、例えば半導体メモリによって構成される。また、メモリ 1 4 1 5 は、ログ領域 1 4 1 5 A と、ライセンス領域 1 4 1 5 B と、データ領域 1 4 1 5 C とから成る。ログ領域 1 4 1 5 A は、ログを記録するための領域である。ログ領域 1 4 1 5 A は、メモリカード 1 1 0 に対してライセンスが入力され、格納されるときに記録される受信ログと、メモリカード 1 1 0 が他のメモリカードに対してライセンスを出力するとき記録される送信ログとから成る。さらに、受信ログは、2 つの状態 (O N, O F F) を持つ受信 s t a t e を含む。

15 受信ログおよび送信ログの詳細については後述する。

ライセンス領域 1 4 1 5 B は、ライセンスを記録するための領域である。ライセンス領域 1 4 1 5 B は、ライセンス (ライセンス鍵 K c、再生制御情報 A C p、アクセス制限情報 A C m、ライセンス I D、コンテンツ I D) と有効フラグとを記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスと有効フラグとを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

20

データ領域 1 4 1 5 C は、暗号化コンテンツデータ {D c} K c、暗号化コンテンツデータ {D c} K c の関連情報 D c - i n f、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、メモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リスト、およびライセンス領域 1 4 1 5 B のエントリを管理するためのエントリ情報を記録するための領域である。そして、データ領域 1 4 1 5 C は、外部から直接アクセスが可能である。ライセンス管理ファ

25

イルおよび再生リストの詳細については後述する。

メモ리카ード110は、さらに、バスBS4を介して外部との間でデータ授受を行ない、バスBS4との間でアクセス制御情報ACm等を受けて、メモ리카ード110の動作を制御するためのコントローラ1420を含む。

- 5       なお、データ領域1415Cを除く全ての構成は、耐タンパモジュール領域に構成される。

- また、図6に示すライセンス専用メモ리카ード520は、メモ리카ード110と同じ構成から成る。ただし、ライセンス専用メモ리카ード520は、メモリ1415内のデータ領域1415Cにエントリ管理情報のみを記録する。そして、
- 10       ライセンス専用メモ리카ード520における自然数wは3以外の値を有し、ライセンス専用メモ리카ード520を識別するための自然数xは4以外の値を持つ。

      以下、図1および図2に示すデータ配信システムにおける各セッションの動作について説明する。

#### [配信]

- 15       まず、図1に示すデータ配信システムにおいて、配信サーバ10から携帯電話機100のメモ리카ード110へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。

- 図9および図10は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機100に装着されたメモ리카ード110へのライセンスの配信動作（以下、配信セッションともいう）を説明するための
- 20       第1および第2のフローチャートである。

- 図9における処理以前に、携帯電話機100のユーザは、配信サーバ10に対して電話網を介して接続し、購入を希望するコンテンツに対するコンテンツIDを取得し、さらに、メモ리카ード110に対するエントリ管理情報を取得してラ
- 25       イセンス領域1415B内の空きエントリを確認していることを前提としている。

      図9を参照して、携帯電話機100のユーザから操作パネル1108を介してコンテンツIDの指定による配信リクエストがなされる（ステップS100）。そして、携帯電話機100のユーザは、操作パネル1108を介して暗号化コン

テンツデータのライセンスを購入するための購入条件ACを入力するように指示し、購入条件ACが入力される（ステップS102）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータのアクセス制御情報ACm、および再生制御情報ACpを設定して購入条件ACが入力される。

暗号化コンテンツデータの購入条件ACが入力されると、コントローラ1106は、バスBS3およびメモリカードインタフェース1200を介してメモリカード110へ認証データの出力指示を与える（ステップS104）。メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する（ステップS106）。そして、コントローラ1420は、バスBS4を介して認証データ保持部1400から認証データ{K P m 3 / / C m 3} K P aを読み出し、認証データ{K P m 3 / / C m 3} K P aをバスBS4、インタフェース1424および端子1426を介して出力する（ステップS108）。

携帯電話機100のコントローラ1106は、メモリカード110からの認証データ{K P m 3 / / C m 3} K P aに加えて、コンテンツID、ライセンス購入条件のデータAC、および配信リクエストを配信サーバ10に対して送信する（ステップS110）。

配信サーバ10は、携帯電話機100から配信リクエスト、コンテンツID、認証データ{K P m 3 / / C m 3} K P a、およびライセンス購入条件のデータACを受信し（ステップS112）、復号処理部312は、メモリカード110から出力された認証データ{K P m 3 / / C m 3} K P aを公開認証鍵K P aで復号する（ステップS114）。

配信制御部315は、復号処理部312における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップS116）。正当な認証データであると判断された場合、配信制御部315は、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を承認し、受理する。そして、次の処理（ステップS118）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m

3およびクラス証明書Cm3を受理しないで配信セッションを終了する（ステップS164）。

5 認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ10において、セッションキー発生部316は、配信のためのセッションキーKs1を生成する（ステップS118）。セッションキーKs1は、復号処理部312によって得られたメモリカード110に対応するクラス公開暗号鍵Kpm3によって、暗号処理部318によって暗号化される（ステップS120）。

10 配信制御部315は、ライセンスIDを生成し（ステップS122）、ライセンスIDおよび暗号化されたセッションキーKs1は、ライセンスID//{Ks1}Km3として、バスBS1および通信装置350を介して携帯電話機100へ送信される（ステップS124）。

15 携帯電話機100が、ライセンスID//{Ks1}Km3を受信すると、コントローラ1106は、ライセンスID//{Ks1}Km3をメモリカード110に入力する（ステップS126）。そうすると、メモリカード110においては、端子1426およびインタフェース1424を介して、コントローラ1420は、ライセンスID//{Ks1}Km3を受理する（ステップS128）。そして、コントローラ1420は、バスBS4を介してメモリ1415のログ領域1415Aに記録されている受信ログを初期化し、受理したライセンスIDをログ領域1415Aに格納する（ステップS130）。このとき、受信ログ内の受信stateは、OFFに設定される。その後、コントローラ1420は、バスBS4を介して暗号化データ{Ks1}Km3を復号処理部1422へ与え、復号処理部1422は、Km保持部1421に保持されるメモリカード110に固有なクラス秘密復号鍵Km3によって復号処理することにより、セッションキーKs1を復号し、セッションキーKs1を受理する（ステップS132）。

25 コントローラ1420は、配信サーバ10で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対してメモリカード110において配信動作時に生成されるセッションキーKs2の生成を指示する。そ

して、セッションキー発生部1418は、セッションキーKs2を生成する（ステップS134）。コントローラ1420は、生成されたセッション鍵Ks2をバスBS4を介して受取り、その受取ったセッション鍵Ks2をメモリ1415のログ領域1415Aに格納し、受信stateをONにする（ステップS136）。

暗号処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1422より与えられるセッションキーKs1によって、切換スイッチ1446の接点を順次切換えることによって与えられるセッションキーKs2、および個別公開暗号鍵KPMC4を1つのデータ列として暗号化して、暗号化データ{Ks2//KPMC4}Ks1をバスBS4に出力する。バスBS4に出力された暗号化データ{Ks2//KPMC4}Ks1は、バスBS4からインタフェース1424および端子1426を介して携帯電話機100に出力され（ステップS138）、携帯電話機100から配信サーバ10に送信される（ステップS140）。

図10を参照して、配信サーバ10は、暗号化データ{Ks2//KPMC4}Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモ리카ード110で生成されたセッションキーKs2、およびメモ리카ード110の個別公開暗号鍵KPMC4を受理する（ステップS142）。

配信制御部315は、ステップS112で取得したコンテンツIDに従ってライセンス鍵Kcを情報データベース304から取得し（ステップS144）、ステップS112で取得したライセンス購入条件ACに従って、アクセス制御情報ACmおよび再生制御情報ACpを決定する（ステップS146）。

配信制御部315は、生成したライセンス、すなわち、ライセンスID、コンテンツID、ライセンス鍵Kc、再生制御情報ACp、およびアクセス制御情報ACmを暗号処理部326に与える。暗号処理部326は、復号処理部320によって得られたメモ리카ード110の個別公開暗号鍵KPMC4によってライセンスを暗号化して暗号化データ{ライセンスID//コンテンツID//Kc//ACm//ACp}KPMC4を生成する（ステップS148）。そして、暗号

処理部 328 は、暗号処理部 326 からの暗号化データ { ライセンス ID // コンテンツ ID // Kc // ACm // ACp } Km c 4 を、復号処理部 320 からのセッションキー K s 2 によって暗号化し、暗号化データ { { ライセンス ID // コンテンツ ID // Kc // ACm // ACp } Km c 4 } K s 2 を出力する。配信制御部 315 は、バス BS 1 および通信装置 350 を介して暗号化データ { { ライセンス ID // コンテンツ ID // Kc // ACm // ACp } Km c 4 } K s 2 を携帯電話機 100 へ送信する (ステップ S 150)。

携帯電話機 100 は、送信された暗号化データ { { ライセンス ID // コンテンツ ID // Kc // ACm // ACp } Km c 4 } K s 2 を受信し、バス BS 3 およびメモ리카ードインタフェース 1200 を介してメモ리카ード 110 に入力する (ステップ S 152)。メモ리카ード 110 においては、端子 1426 およびインタフェース 1424 を介して、バス BS 4 に与えられた受信データを復号処理部 1412 によって復号する。復号処理部 1412 は、セッションキー発生部 1418 から与えられたセッションキー K s 2 を用いてバス BS 4 の受信データを復号し、バス BS 4 に出力する (ステップ S 154)。

この段階で、バス BS 4 には、Km c 保持部 1402 に保持される個別秘密復号鍵 Km c 4 で復号可能な暗号化ライセンス { ライセンス ID // コンテンツ ID // Kc // ACm // ACp } Km c 4 が出力される (ステップ S 154)。

コントローラ 1420 の指示によって、暗号化ライセンス { ライセンス ID // コンテンツ ID // Kc // ACm // ACp } Km c 4 は、復号処理部 1404 において、個別秘密復号鍵 Km c 4 によって復号され、ライセンス (ライセンス鍵 Kc、ライセンス ID、コンテンツ ID、アクセス制御情報 ACm および再生制御情報 ACp) が受理される (ステップ S 156)。

携帯電話機 100 のコントローラ 1106 は、メモ리카ード 110 のメモリ 1415 から読出したエントリ管理情報に基づいて、配信サーバ 10 から受信したライセンスを格納するためのエントリ番号を決定し、その決定したエントリ番号をバス BS 3 およびメモ리카ードインタフェース 1200 を介してメモ리카ード 110 へ入力する (ステップ S 158)。

そうすると、メモリカード110のコントローラ1420は、端子1426およびインタフェース1424を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ1415のライセンス領域1415Bに、ステップS156において取得したライセンス（ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp）を格納し、同一エントリにおける有効フラグを有効にする（ステップS160）。そして、コントローラ1420は、バスBS4を介してメモリ1415のログ領域1415Aの受信ログに記録された受信stateをOFFする（ステップS161）。ライセンスの書込みが終了すると、コントローラ1106は、ステップS158においてメモリカード110へ入力したエントリが使用中であるようにエントリ管理情報を更新し、その更新したエントリ管理情報をメモリカード110へ入力する（ステップS162）。メモリカード110のコントローラ1420は、入力されたエントリ管理情報を用いてメモリ1415のデータ領域1415C内にエントリ管理情報を書換える（ステップS163）。そして、ライセンスの配信動作が終了する（ステップS164）。

ライセンスの配信セッションが終了した後、携帯電話機100のコントローラ1106は、暗号化コンテンツデータの配信要求を配信サーバ10へ送信し、配信サーバ10は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ10の配信制御部315は、情報データベース304より、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得して、これらのデータをバスBS1および通信装置350を介して携帯電話機100へ送信する。

携帯電話機100は、データ{Dc}Kc//Dc-infを受信して、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを受理する。そうすると、コントローラ1106は、暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを1つのコンテンツファイルとしてバスBS3およびメモリカードインタフェース1200を介してメモリカード110に入力する。また、コントローラ1106は、メモリカード110に格納されたライセンスのエントリ番号と、平文のライセンスIDと、コンテンツIDとを含み、かつ、暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとに対するライセンス

管理ファイルを生成し、その生成したライセンス管理ファイルをバス B S 3 およびメモ리카ードインタフェース 1 2 0 0 を介してメモ리카ード 1 1 0 に入力する。さらに、コントローラ 1 1 0 6 は、メモ리카ード 1 1 0 のメモリ 1 4 1 5 に記録されている再生リストに、受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や付加情報 D c - i n f から抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し、全体の処理が終了する。

このようにして、携帯電話機 1 0 0 に装着されたメモ리카ード 1 1 0 が正規の認証データを保持する機器であること、同時に、クラス証明書 C m 3 とともに暗号化して送信できた公開暗号鍵 K P m 3 が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモ리카ードへのコンテンツデータの配信を禁止することができる。

さらに、配信サーバおよびメモ리카ードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

また、メモ리카ード 1 1 0 は、配信サーバ 1 0 から暗号化コンテンツデータおよびライセンスを受信する際に、配信サーバ 1 0 との間でハード的にデータのやり取りを行ない、暗号化コンテンツデータを再生するためのライセンスをハード的に格納するため、そのセキュリティレベルは高い。

図 6 に示すライセンス専用メモ리카ード 5 2 0 へのライセンスの配信動作も図 9 および図 1 0 に示すフローチャートに従って行なわれる。また、ライセンス専用メモ리카ード 5 2 0 への暗号化コンテンツデータの配信動作も上述したのと同じ動作によって行なわれる。すなわち、上記の説明において、携帯電話機 1 0 0 をパーソナルコンピュータ 5 0 に代え、メモ리카ード 1 1 0 をライセンス専用メモ리카ード 5 2 0 に代えれば良い。その他は、上述したのと同じである。

ライセンス専用メモ리카ード 5 2 0 への暗号化コンテンツデータおよびライセンスの配信においても暗号化コンテンツデータおよびライセンスをハード的に受



信し、かつ、格納するので、ライセンス専用メモ리카ード520への暗号化コンテンツデータおよびライセンスの配信は、メモ리카ード110への暗号化コンテンツデータおよびライセンスの配信と同じようにセキュリティレベルが高い。

図11を参照して、パーソナルコンピュータ50のライセンス専用メモ리카ード520によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ50のハードディスク530は、再生リスト150と、コンテンツファイル1531～1535と、ライセンス管理ファイル1521～1525とを含む。

再生リスト150は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報（楽曲名、アーティスト名など）と、コンテンツファイルとライセンス管理ファイルとを示す情報（ファイル名）などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Dc-infから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、またはライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

コンテンツファイル1531～1535は、ライセンス管理デバイス520によって受信された暗号化コンテンツデータ {Dc} Kcと付加情報Dc-infとを記録するファイルであり、コンテンツごとに設けられる。

また、ライセンス管理ファイル1521～1525は、それぞれ、コンテンツファイル1531～1535に対応して記録されており、ライセンス専用メモ리카ード520に受信され、記録されているライセンスを管理するためのファイルである。これまでの説明でも明らかなように、ライセンスは通常参照することができないが、ライセンス鍵Kcを除く他の情報は、ユーザが書き換えることさえできなければ著作権保護の点では問題ない。しかし、運用においてライセンス鍵Kcと分離して管理することはセキュリティの低下につながるため好ましくない。そこで、ライセンスの配信を受ける場合に平文にて参照できるライセンスID、コンテンツIDや、ライセンス購入条件ACから容易に判断できるアクセス制御情報ACmおよび再生制御情報ACpにて制限されている事項の写しを平文にて記録する。さらに、ライセンス専用メモ리카ード520にライセンスが記録

された場合にエントリ番号を記録する。ライセンス専用メモ리카ード520のメモリ5215のライセンス領域525Bは、高いセキュリティレベルでライセンスを記録する耐タンパモジュールで構成された記録領域である。ライセンス（ライセンス鍵Kc、再生制御情報ACp、アクセス制限情報ACm、ライセンスID）を記録するためにM個のエントリを備えている。

ライセンス管理ファイル1521, 1524, 1522, 1525は、それぞれ、エントリ番号0, 1, 2, 3, を含む。これは、ライセンス専用メモ리카ード520によって受信され、ライセンス専用メモ리카ード520のメモリ5215のライセンス領域5215Bにおいて管理されるライセンス（ライセンスID、ライセンス鍵Kc、アクセス制御情報ACmおよび再生制御情報ACm）の管理領域を指定する番号である。

また、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを携帯電話機100または再生端末102に装着されたメモ리카ード110へ移動させるとき、コンテンツファイル1531～1535を検索してコンテンツファイル1531を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル1531に対応するライセンス管理ファイル1521に含まれるエントリ番号は「0」であるので、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス専用メモ리카ード520のメモリ5215のライセンス領域5215Bのエントリ番号0によって指定された領域に記録されている。そうすると、ハードディスク530に記録された再生リストファイル150のライセンス管理ファイル1521からエントリ番号0を読み出し、その読み出したエントリ番号0をライセンス専用メモ리카ード520に入力することによって、メモリ5215のライセンス領域5215Bからライセンスを容易に取出し、メモ리카ード110へ移動できる。そして、ライセンスを移動した後は、メモリ5215のライセンス領域5215Bにおいて指定されたエントリ番号内の有効フラグは無効になり、それに対応してライセンス管理ファイル1523のように「ライセンス無」が記録される。

ライセンス管理ファイル1523は、「ライセンス無」を含む。これは、ライ

センス専用メモリカード520によって受信されたライセンスが、メモリカードや他のライセンス専用メモリカードへ移動された結果である。対応するコンテンツファイル1533はハードディスク530に記録されたままになっている。メモリカードや他のライセンス専用メモリカードからライセンスを再びライセンス専用メモリカード520へ移動、あるいは、配信サーバ10から再び配信を受ける場合には、ライセンスについてのみ配信を受けることが可能である。また、エントリ管理情報155がライセンス専用メモリカード520のデータ領域5215Cに記録されている。エントリ管理情報155は、ライセンス専用メモリカード520のライセンス領域5215Bのエントリの使用状態を示す情報である。

したがって、エントリ管理情報155を参照すれば、エントリの使用状態が解かる。

図12は、メモリカード110のメモリ1415におけるライセンス領域1415Bとデータ領域1415Cとを示したものである。データ領域1415Cには、再生リストファイル160と、エントリ管理情報165と、コンテンツファイル1611~161nと、ライセンス管理ファイル1621~162nとが記録されている。コンテンツファイル1611~161nは、受信した暗号化コンテンツデータ {Dc} Kcと付加情報Dc-infとを1つのファイルとして記録する。また、ライセンス管理ファイル1621~162nは、それぞれ、コンテンツファイル1611~161nに対応して記録されている。

メモリカード110は、配信サーバ10から暗号化コンテンツデータおよびライセンスを受信したとき、パーソナルコンピュータ50から暗号化コンテンツデータおよびライセンスを「移動セッション」によって受信したとき、暗号化コンテンツデータおよびライセンスをメモリ1415に記録する。

したがって、パーソナルコンピュータ50のライセンス専用メモリカード520によって受信され、かつ、移動セッションによってメモリカード110に送信されたセキュリティレベルの高い暗号化コンテンツデータのライセンスは、メモリ1415のライセンス領域1415Bのエントリ番号によって指定された領域に記録され、メモリ1415のデータ領域1415Cに記録された再生リストファイル160のライセンス管理ファイルを読出せば、エントリ番号を取得でき、

その取得したエントリ番号によって対応するライセンスをライセンス領域 1 4 1 5 B から読出すことができる。

また、ライセンス管理ファイル 1 6 2 2 は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル 1 6 1 2 は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、再生端末が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

また、コンテンツファイル 1 6 1 3 は、点線で示されているが、これは、たとえば、再生端末が配信サーバ 1 0 から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけを他の携帯電話機へ送信した場合に相当し、ライセンスはメモリ 1 4 1 5 に存在するが暗号化コンテンツデータが存在しないことを意味する。

#### [移動／複製]

上述したように、図 1 に示すデータ配信システムにおいて、携帯電話機 1 0 0 に装着されたメモリカード 1 1 0 は、携帯電話網を介して配信サーバ 1 0 からライセンスを受信して記録することができる。また、図 1 および図 2 に示すデータ配信システムにおいて、パーソナルコンピュータ 5 0 に装着されたライセンス専用メモリカード 5 2 0 は、インターネット網 3 0 を介して配信サーバ 1 0 からライセンスを受信して記録することができる。

また、図 1 および図 2 のデータ配信システムにおけるメモリカード 1 1 0 またはライセンス専用メモリカード 5 2 0 は、記録されているライセンスを他のメモリカード（ライセンス専用メモリカードを含む）に安全に移動／複製させるための機能を備えており、記録されているライセンスを他のメモリカードに移動／複製することができる。当然のことながら、メモリカード 1 1 0 とライセンス専用メモリカード 5 2 0 との間においてもライセンスの移動／複製を行なうことができる。

したがって、図 1 および図 2 に示すデータ配信システムでは、パーソナルコンピュータ 5 0 に装着されたライセンス専用メモリカード 5 2 0 に記録されたライセンスを携帯電話機 1 0 0 または再生端末 1 0 2 に装着されたメモリカード 1 1 0 へ移動／複製させることができる。また、逆に、携帯電話機 1 0 0 または再生

端末 102 に装着されたメモリカード 110 に記録されたライセンスをパーソナルコンピュータ 50 に装着されたライセンス専用メモリカード 520 に移動／複製させることができる。その結果、ユーザの利便性の向上を図ることができる。

5 また、暗号化コンテンツデータは、自由にアクセス可能なパーソナルコンピュータ 50 のハードディスク 530 またはメモリカード 110 のデータ領域 1415 C に記録されているので自由に複製可能であるが、ライセンスの移動／複製が伴わなければ再生することができない。

そこで、メモリカード 110 またはライセンス専用メモリカード 520 に記録されているライセンスを他のメモリカードに移動／複製するときの動作について  
10 説明する。

この場合、図 8 に示す構成を有する 2 つのメモリカード間でライセンスの移動／複製が行なわれ、パーソナルコンピュータ 50、携帯電話機 110 および再生  
端末 102 は、それぞれ、装着されたメモリカード（ライセンス専用メモリカードを含む）に対するデータの入出力処理と通信路を提供し、データの中継処理を  
15 行なうのみであるため説明を簡単にするために図 13 に示すような系を考える。

図 13 に示す系は、コントローラ 40 と、メモリカードを制御するインタフェース 60 と、2 枚のメモリカード 110、120 によって構成される。図 1 に示すデータ配信システムを想定するとパーソナルコンピュータ 50 に装着されたライセンス専用メモリカード 520 から携帯電話機 100 に装着されたメモリカード 110 に、または携帯電話機 100 に装着されたメモリカード 110 からパーソナルコンピュータ 50 に装着されたライセンス専用メモリカード 520 に、ライセンスを移動／複製することを想定すると、メモリカード 120 はライセンス専用メモリカード 520、インタフェース 60 はパーソナルコンピュータ 50 のメモリカードインタフェース 525 および携帯電話機 100 のメモリカードインタフェース 1200 に相当する。さらに、コントローラ 40 は、パーソナルコンピュータ 50 のコントローラ 510 および携帯電話機 100 のコントローラ 1106 の機能を行ない、パーソナルコンピュータ 50 と携帯電話機 100 との間の通信に関する部分を省略したものである。また、図 2 に示すデータ配信システムを想定する場合には、携帯電話機 100 を再生端末 102 に読替えればよい。

また、図 1 に示すデータ配信システムにおいて、携帯電話機 100 が公衆網を介して他の携帯電話機に対してライセンスの移動／複製を行なうことも可能である。さらに、図 1 および図 2 に示すデータ配信システムにおける携帯電話機 100 または再生端末 102 が端末間の独自の通信手段を備え、携帯電話機 100 または再生端末 102 から他の携帯電話機または再生端末へライセンスの移動／複製を行なうことも可能である。この場合、メモ리카ード 120 は、他の携帯電話機または再生端末に装着されたメモ리카ードに相当する。インタフェース 60 は、携帯電話機 100 または再生端末 102 のメモ리카ードインタフェース 1200 と通信相手である他の携帯電話機または再生端末のメモ리카ードインタフェースに相当する。コントローラ 40 は、携帯電話機 100 または再生端末 102 のコントローラ 1106 と通信相手である他の携帯電話機または再生端末のコントローラに相当する。そして、図 13 においては、通信手段を用いた通信に関する部分を省略したものである。

さらに、図 7 に示した再生端末 102 は、メモ리카ードを 1 枚装着する構成であるが、2 枚以上のメモ리카ードを装着するような構成にすることも可能である。この場合、コントローラ 40 は、再生端末 102 のコントローラ 1106 に相当し、インタフェース 60 は、2 枚以上装着できるように変更したメモ리카ードインタフェース 1200 に相当する。携帯電話機 100 においても、2 枚以上のメモ리카ードを装着可能な構成に変更することも可能である。その場合、再生端末 102 を携帯電話機 100 に読替えばよい。

また、さらに、メモ리카ード 110 へのデータの書込みおよび読出しを行なうメモ리카ードライターやパーソナルコンピュータに装着されたメモ리카ードドライバ装置を用いてライセンスの移動／複製を行なう系を構成することも可能である。

図 14～図 16 は、図 13 におけるメモ리카ード 120 に記録されたライセンスをメモ리카ード 110 に移動／複製するためのフローチャートである。なお、図 14 における処理以前に、コントローラ 40 は、ユーザがライセンスの移動／複製を行なうコンテンツの指定およびライセンスの移動／複製リクエストを行なうための入力手段（図示せず）に接続され、ユーザによってなされたライセンス

の移動／複製を行なうコンテンツの指定、およびライセンスの移動／複製リクエストを受取る。そして、コントローラ 40 は、送信側であるメモ리카ード 120 内の再生リストを参照してライセンスの移動／複製を行なうライセンス管理ファイルを取得していることを前提としている。また、送信側のメモ리카ード 120  
5 および受信側のメモ리카ード 110 内に格納されている、それぞれのエントリ管理情報を取得していることを前提としている。さらに、受信側のメモ리카ード 120 に格納されたエントリ管理情報によって、受信側のメモ리카ード 110 のライセンス領域 1415B 内に空きのエントリを確認していることを前提としている。

10 図 14 を参照して、移動／複製リクエストがユーザから指示されると（ステップ S300）、コントローラ 40 は、メモ리카ード 110 へ認証データの送信要求をインタフェース 60 を介してメモ리카ード 110 へ送信する（ステップ S302）。そして、メモ리카ード 110 のコントローラ 1420 は、端子 1426、インタフェース 1424 およびバス BS4 を介して認証データの送信要求を受信する（ステップ S304）。  
15

メモ리카ード 110 のコントローラ 1420 は、認証データの送信要求を受信すると、認証データ保持部 1400 から認証データ {K P m 3 / / C m 3} K P a をバス BS4 を介して読出し、その読出した認証データ {K P m 3 / / C m 3} K P a をバス BS4、インタフェース 1424 および端子 1426 を介して  
20 インタフェース 60 へ出力する（ステップ S306）。そして、コントローラ 40 は、インタフェース 60 を介して認証データ {K P m 3 / / C m 3} K P a を受取り、インタフェース 60 を介してメモ리카ード 120 へメモ리카ード 110 の認証データ {K P m 3 / / C m 3} K P a を送信する（ステップ S308）。

そうすると、メモ리카ード 120 のコントローラ 1420 は、端子 1426 およびインタフェース 1424 を介して認証データ {K P m 3 / / C m 3} K P a  
25 を受信し、その受信した認証データ {K P m 3 / / C m 3} K P a をバス BS4 を介して復号処理部 1408 へ与える。そして、復号処理部 1408 は、K P a 保持部 1414 からの公開認証鍵 K P a によって認証データ {K P m 3 / / C m 3} K P a の復号処理を実行する（ステップ S310）。コントローラ 1420

- は、復号処理部 5 2 0 8 における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード 1 1 0 が正規のメモリカードであって、メモリカード 1 1 0 から正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップ S 3 1 2）。正当な
- 5 認証データであると判断された場合、コントローラ 1 4 2 0 は、認証データから取得されたクラス公開暗号鍵 K P m 3 およびクラス証明書 C m 3 を承認し、受理する。そして、次の処理（ステップ S 3 1 4）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵 K P m 3 およびクラス証明書 C m 3 を受理しないで処理を終了する（ステップ S 3 7 0）。
- 10 認証の結果、正当な認証データを持つメモリカードへのライセンスの移動／複製であることが確認されると、メモリカード 1 2 0 において、コントローラ 1 4 2 0 は、セッションキー発生部 1 4 1 8 を制御し、セッションキー発生部 1 4 1 8 は、移動のためのセッションキー K s 2 a を生成する（ステップ S 3 1 4）。セッションキー K s 2 a は、復号処理部 1 4 0 8 によって得られたメモリカード
- 15 1 1 0 に対応するクラス公開暗号鍵 K P m 3 によって、暗号処理部 1 4 1 0 によって暗号化される。そして、メモリカード 1 2 0 のコントローラ 1 4 2 0 は、バス B S 4 を介して暗号化データ {K s 2 a} K m 3 を取得し、バス B S 4、インタフェース 1 4 2 4 および端子 1 4 2 6 を介してインタフェース 6 0 に出力する（ステップ S 3 1 6）。
- 20 コントローラ 4 0 は、インタフェース 6 0 を介して暗号化データ {K s 2 a} K m 3 を送信側から受理し（ステップ S 3 1 8）、送信側のメモリカード 1 2 0 のライセンス管理情報からライセンス ID を取得する（ステップ S 3 2 0）。そして、コントローラ 4 0 は、取得したライセンス ID と、ステップ S 3 1 8 において受理した暗号化データ {K s 2 a} K m 3 とを 1 つにデータにしてライセン
- 25 ス ID／／ {K s 2 a} K m 3 をインタフェース 6 0 を介してメモリカード 1 1 0 へ入力する（ステップ S 3 2 2）。そうすると、メモリカード 1 1 0 のコントローラ 1 4 2 0 は、端子 1 4 2 6、インタフェース 1 4 2 4、およびバス B S 4 を介してライセンス ID／／ {K s 2 a} K m 3 を受理する。そして、メモリカード 1 1 0 のコントローラ 1 4 2 0 は、メモリ 1 4 1 5 のログ領域 1 4 1 5 A を



初期化し、受理したライセンスIDをログ領域1415Aに格納する（ステップS326）。この受信ログの初期化によって暗号化コンテンツデータのライセンスの配信時に格納されたライセンスIDおよびセッションキーKs2（図9のステップS130, S136）が消去され、受信stateがOFFされる。その後、コントローラ1420は、暗号化データ{Ks2a} Km3を復号処理部1422へ与え、復号処理部1422は、Km保持部1421からのクラス秘密復号鍵Km3によって暗号化データ{Ks2a} Km3を復号してセッションキーKs2aを受理する（ステップS328）。そして、セッションキー発生部1418は、セッションキーKs2bを生成し（ステップS330）、コントローラ1420は、バスBS4を介してセッションキーKs2bを受取り、その受取ったセッションキーKs2bをメモリ1415のログ領域1415Aの受信ログに格納して受信stateをONにする（ステップS332）。このセッションキーKs2bの格納によってメモ리카ード120からメモ리카ード110へのライセンスの移動／複製処理を特定するための履歴情報が受信ログに記録されたことになる。

そうすると、メモ리카ード110の暗号処理部1406は、切換スイッチ1446の端子を順次切換えることによって、セッションキー発生部1418で発生されたセッションキーKs2b、および個別公開暗号鍵Kpmc4を、復号処理部1404によって復号されたセッションキーKs2aによって暗号化し、暗号化データ{Ks2b／／Kpmc4} Ks2aを生成する。メモ리카ード120のコントローラ1420は、暗号化データ{Ks2b／／Kpmc4} Ks2aをバスBS4、インタフェース1424および端子1426を介してインタフェース60へ出力する（ステップS334）。

コントローラ40は、メモ리카ード110からインタフェース60を介して暗号化データ{Ks2b／／Kpmc4} Ks2aを受理する。そして、コントローラ40は、暗号化データ{Ks2b／／Kpmc4} Ks2aをインタフェース60を介してメモ리카ード120へ送信する（ステップS334）。なお、ステップS334において、暗号化データ{Ks2b／／Kpmc4} Ks2aがメモ리카ード110から出力された時点で、メモ리카ード110とメモ리카ード

1 2 0との間にライセンスの移動／複製のための通信が確立されたことになる。

図15を参照して、メモ리카ード120のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して暗号化データ {K s 2 b／／K P m c 4} K s 2 aを受信し、その受信した暗号化データ {K s 2 b／／K P m c 4} K s 2 aを復号処理部1412に与える。復号処理部1412は、セッションキー発生部1418からのセッションキーK s 2 aによって暗号化データ {K s 2 b／／K P m c 4} K s 2 aを復号し、セッションキーK s 2 b、および公開暗号鍵K P m c 4を受信する（ステップS338）。

そうすると、メモ리카ード120のコントローラ1420は、メモリ1415のログ領域1415Aに含まれる送信ログを初期化し、受理したセッションキーK s 2 bを送信ログに格納する（ステップS340）。これによって、メモ리카ード120からメモ리카ード110へのライセンスの移動／複製処理を特定するための履歴情報であるセッションキーK s 2 bが送信ログに記録されたことになる。

その後、コントローラ40は、送信側であるメモ리카ード120のライセンス管理情報から移動／複製の対象となっているライセンスが格納されているエントリ番号を取得し（ステップS342）、その取得したエントリ番号をインタフェース60を介してメモ리카ード120へ送信する（ステップS344）。メモ리카ード120のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介してエントリ番号を受信し、その受信したエントリ番号によって指定されるメモリ1415のライセンス領域1415Bのエントリからライセンス（ライセンスID、コンテンツID、ライセンス鍵K c、アクセス制御情報AC m、再生制御情報AC p）と有効フラグとを取得する（ステップS346）。

コントローラ1420は、有効フラグの確認を行なう（ステップS347）。有効フラグが有効な場合には、次のステップS348へ進む。有効フラグが無効な場合には、指定されたライセンスが、すでに移動済みであり、ライセンスが使用不能になっていることを示しているためステップS370へ移行し、移動／複製動作を終了する。ステップS347において有効フラグが有効な場合、コント

- ローラ 1 4 2 0 は、アクセス制御情報 A C m を確認する（ステップ S 3 4 8）。つまり、コントローラ 1 4 2 0 は、取得したアクセス制御情報 A C m に基づいて、最初に、メモ리카ード 1 1 0 へ移動／複製しようとするライセンスが再生回数によって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数が残っていない場合（再生回数＝0）、暗号化コンテンツデータをライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとをメモ리카ード 1 1 0 へ移動する意味がないからである。再生することができる場合、移動・複製フラグによって、ライセンスの複製、移動の可否を判断する。
- 10        ステップ S 3 4 8 において、暗号化コンテンツデータの再生ができない（再生回数＝0）、または、移動・複製フラグが移動複製禁止（＝0）の場合、アクセス制御情報 A C m によって、複製移動不可と判断し、ステップ S 3 7 0 へ移行し、移動／複製動作は終了する。ステップ S 3 4 8 において、暗号化コンテンツデータの再生ができ（再生回数≠0）、かつ、移動・複製フラグが移動のみ可
- 15        「＝1」の場合、ライセンスの移動であると判断され、コントローラ 1 4 2 0 は、メモリ 1 4 1 5 のライセンス領域 1 4 1 5 B において指定されたエントリ番号内の有効フラグを無効にし、そのエントリ番号を送信ログに格納する（ステップ S 3 5 0）。また、暗号化コンテンツデータの再生ができ「再生回数≠0」、かつ、移動・複製フラグが移動複製可「＝3」の場合、ライセンスの複製であると判断され、ステップ S 3 5 0 を行なわずにステップ S 3 5 2 へ移行する。
- 20        ステップ S 3 4 8 またはステップ S 3 5 0 の後、メモ리카ード 1 2 0 の暗号処理部 1 4 1 7 は、復号処理部 1 4 1 2 によって得られたメモ리카ード 1 1 0 に固有の公開暗号鍵 K P m c 4 によってライセンスを暗号化して暗号化データ {ライセンス I D // コンテンツ I D // K c // A C m // A C p } K m c 4 を生成
- 25        し（ステップ S 3 5 2）、暗号処理部 1 4 0 6 は、暗号処理部 1 4 1 7 によって暗号化された暗号化データ {ライセンス I D // コンテンツ I D // K c // A C m // A C p } K m c 4 をスイッチ 1 4 4 6 の接点 P c を介して受取り、復号処理部 1 4 1 2 によって復号されたセッションキー K s 2 b をスイッチ 1 4 4 2 の接点 P b を介して受取り、暗号化データ {ライセンス I D // コンテンツ I D

5 //Kc//ACm//ACp} Km c 4をセッションキーK s 2 bによって暗号化する。そして、メモ리카ード1 2 0のコントローラ1 4 2 0は、暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bをバスBS 4、インタフェース1 4 2 4、および端子1 4 2 6を介して出力する (ステップS 3 5 4)。

10 このように、ライセンスを移動するときは、ライセンス領域1 4 1 5 Bの有効フラグを無効にしてから (ステップS 3 5 0参照)、ステップS 3 5 2の処理を行なうが、ライセンスを複製するときは、複製元と複製先との両方においてライセンスを使用可能にするためにライセンスの有効フラグを無効にするステップS 3 5 0を介さずに有効フラグを有効なままステップS 3 5 2へ移行するようにしたものである。したがって、ライセンスを移動させたときは、送信側のメモ리카ード1 2 0からライセンスを読出すことはできなり、ライセンスを消去した場合と同様な扱いとなる。

15 図1 6を参照して、コントローラ4 0は、インタフェース6 0を介してメモ리카ード1 2 0から暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bを受理し、その受理した暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bをメモ리카ード1 1 0へ入力する (ステップS 3 5 6)。

20 メモ리카ード1 1 0のコントローラ1 4 2 0は、端子1 4 2 6、インタフェース1 4 2 4、およびバスBS 4を介して暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bの入力を受けて、暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bを復号処理部1 4 1 2へ与える。そして、復号処理部1 4 1 2は、暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bをバスBS 4を介して受取り、セッションキー発生部1 4 1 8によって発生されたセッションキーK s 2 bによって復号し、暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bを受理する (ステップS 3 5 8)。

その後、コントローラ1 4 2 0の指示によって、暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bをバスBS 4を介して受取り、セッションキー発生部1 4 1 8によって発生されたセッションキーK s 2 bによって復号し、暗号化データ { {ライセンスID//コンテンツID//Kc//ACm//ACp} Km c 4} K s 2 bを受理する (ステップS 3 5 8)。

D//コンテンツID//Kc//ACm//ACp} Km c 4は、復号処理部1404において、秘密復号鍵Km c 4によって復号され、ライセンス（ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp）が受理される（ステップS360）。

- 5       そうすると、コントローラ40は、受信側であるメモ리카ード110のエントリ管理情報を参照して空きのエントリ番号を取得し、その取得したエントリ番号を移動/複製されたライセンスを格納するためのエントリ番号としてメモ리카ード110に入力する（ステップS362）。

- 10       メモ리카ード110のコントローラ1420は、端子1426およびインタフェース1424を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ1415のライセンス領域1415Bに、ステップS360において受理したライセンス（ライセンス鍵Kc、ライセンスID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp）を格納し、同一エントリの有効フラグを有効にする（ステップS364）。そして、コントローラ
- 15       1420は、ログ領域1415Aに含まれる受信ログに記録された受信stateをOFFにする（ステップS366）。その後、コントローラ40は、受信側のメモ리카ード110に対するエントリ管理情報を更新し（ライセンスを記録したエントリを使用中に変更）、受信側のメモ리카ード110に入力する（ステップS367a）。受信側のメモ리카ード110のコントローラ1420は、入力
- 20       されたエントリ管理情報を用いて、メモリ1415のデータ領域1415C内のエントリ管理情報を書換える（ステップS367b）。次に、コントローラ40は、ライセンスの移動であったかライセンスの複製であったかを判断する（ステップS368）。複製処理である場合には、ここで、ライセンスの複製の処理を終了する（ステップS370）。移動処理である場合には、コントローラ40
- 25       は、送信側のメモ리카ード120に対するエントリ管理情報を更新し（移動させたライセンスが格納されたエントリを未使用に変更）、送信側のメモ리카ード120に入力する（ステップS369a）。送信側のメモ리카ード120のコントローラ1420は、入力されたエントリ管理情報を用いて、メモリ1415のデータ領域1415C内のエントリ管理情報を書換える（ステップS369b）。

そして、ライセンスの移動の処理を終了する（ステップS 3 7 0）。

5       なお、暗号化コンテンツデータのメモリカード1 2 0からメモリカード1 1 0への移動／複製は、ライセンスの移動／複製が終了した後、メモリカード1 2 0のデータ領域1 4 1 5 Cから暗号化コンテンツデータを読み出してメモリカード1 1 0へ送信することによって行なえば良い。

10       また、受信側のメモリカード1 1 0に対しては、移動／複製したライセンスに対するライセンス管理ファイルがすでに記録されている場合には、ライセンス管理ファイルに対してエントリ番号などの書込みを行なうことで対象のライセンス管理ファイルを更新する。また、対象となるライセンス管理ファイルがメモリカード1 1 0に記録されていない場合には、新たにライセンス管理ファイルを生成し、その生成したライセンス管理ファイルを受信側のメモリカード1 1 0に記録する。このとき、受信側のメモリカードが図1および図2に示すデータ配信システムにおけるライセンス専用メモリカード5 2 0であるとする、ライセンス管理情報はハードディスク5 3 0に記録される。

15       このようにして、再生端末1 0 2に装着されたメモリカード1 1 0が正規の機器であること、同時に、クラス証明書C m 3とともに暗号化して送信できた公開暗号鍵K P m 3が有効であることを確認した上で、正規なメモリカードへの移動要求に対してのみライセンスを移動することができ、不正なメモリカードへの移動を禁止することができる。

20       また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの移動／複製の動作におけるセキュリティを向上させることができる。

25       上記においては、メモリカード間における暗号化コンテンツデータのライセンスの移動／複製の動作を説明したが、パーソナルコンピュータ5 0のライセンス専用メモリカード5 2 0からメモリカード1 1 0へのライセンスの移動／複製も図1 4および図1 5に示すフローチャートに従って行なうことができる。この移動／複製の動作を用いることによって、配信サーバ1 0との通信機能を有さない

再生端末 102 のユーザも、パーソナルコンピュータ 50 を介して暗号化コンテンツデータのライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

5 また、メモリカード 110 からライセンス専用メモリカード 520 へのライセンスの移動も、図 14～図 16 に示すフローチャートに従って行なわれる。つまり、図 1 において、携帯電話機 100 によって配信を受け、メモリカード 110 に格納した暗号化コンテンツデータとライセンスとをパーソナルコンピュータ 50 へ退避できることになる。

10 図 17 を参照して、ログ領域 1415A に格納される受信ログと送信ログとについて説明する。ライセンス領域 1415B には、エントリ番号 0～N-1 に対応してライセンス ID、コンテンツ ID、ライセンス鍵 Kc、アクセス制限情報 ACm、再生制御情報 ACp、および有効フラグが格納されている。有効フラグは、ライセンス（ライセンス ID、コンテンツ ID、ライセンス鍵 Kc、アクセス制限情報 ACm、および再生制御情報 ACp）の有効性を示すフラグであり、  
15 有効フラグが「有効」であるとき、このライセンスを用いて再生を行ったり、このライセンスを他のメモリカード 110 またはライセンス専用メモリカード 520 へ移動／複製できることを意味し、有効フラグが「無効」であるとき、このライセンスを用いて再生できず、かつ、ライセンスを他のメモリカード 110 またはライセンス専用メモリカード 520 へ移動／複製できないことを意味する。  
20 すなわち、ライセンスが存在しないことと同等の意味を持つ。移動の対象となったライセンスをメモリカード 120 から取得した後、ライセンス領域 1415B の有効フラグを無効にしている（図 15 のステップ S350）のは、メモリカード 120 からメモリカード 110 へライセンスを移動した後はメモリカード 120 において移動の対象となったライセンスを使用できないようにするためである。  
25

また、ログ領域 1415A には、受信ログ 70 および送信ログ 80 が記録されている。受信ログ 70 は、ライセンス ID 71、セッションキー 72 および受信 state 73 から成る。また、送信ログ 80 は、セッションキー 81 およびエントリ番号 82 とから成る。受信ログ 70 は、メモリカード 110 またはライセ

5       ンス専用メモリカード520が配信サーバ10、または他のメモリカードやライセンス専用メモリカードからライセンスを受信するときに、その通信履歴を記録しておくものである。送信ログ80は、ライセンスを他のメモリカードまたはライセンス専用メモリカードへ移動／複製するときに、その通信履歴を記録しておくものである。

10       なお、ライセンス領域1415Bおよびログ領域1415Aは、TRM領域に設けられていることが好ましい。また、ログ領域1415A、ライセンス領域1415Bおよびデータ領域1415Cは、メモリ1415として1つの領域に含まれている必要はなく、それぞれ、独立した構成であってもよい。さらに、ログ領域1415Aに記録された受信ログ70および送信ログ80は、外部から書換えができないように構成されていなければならない。

15       メモリカード110またはライセンス専用メモリカード520が配信サーバ10からライセンスを受信するときに、ライセンスID、および自己のセッションキー発生部1418で生成したセッションキーを受信ログ70に記録し（図9のステップS130、およびステップS136参照）、受信ログ70に記録された受信state73をONにしている（図9のステップS136参照）。また、メモリカード110またはライセンス専用メモリカード520が他のメモリカードまたはライセンス専用メモリカードからライセンスを受信するときに、同様に、

20       ライセンスID、および自己のセッションキー発生部1418で生成したセッションキーを受信ログ70に記録し（図14のステップS326、およびステップS332参照）、受信stateをONにしている（図14のステップS332参照）。

25       一方、図13におけるメモリカード120からメモリカード110へのライセンスの移動において、受信側のメモリカード110から送信されたセッションキーおよび移動／複製の対象となったライセンスのエントリ番号を送信ログ80に記録する（図15のステップS340およびステップS350参照）。メモリカード120からメモリカード110への移動／複製処理においては、受信ログ70のセッションキー72と送信ログ80のセッションキー81とは同じセッションキーKs2bが記録される（図14のステップS332および図15のステ



ップS 3 4 0参照)。したがって、メモ리카ード1 2 0からメモ리카ード1 1 0へのライセンスの移動/複製の途中において通信が切断されたとき、メモ리카ード1 2 0の送信ログ8 0に記録されたセッションキー8 1が、メモ리카ード1 1 0の受信ログ7 0に記録されたセッションキー7 2に一致することを確認すれば、メモ리카ード1 2 0からメモ리카ード1 1 0へのライセンスの移動/複製処理を特定することができる。

また、メモ리카ード1 1 0へのライセンスの配信においては、メモ리카ード1 1 0が、メモ리카ード1 1 0において生成したセッションキーK s 2を配信サーバ1 0へ送信すると、受信s t a t e 7 3がONされ(図9のステップS 1 3 8)、配信サーバ1 0から受信したライセンスをメモリ1 4 1 5のライセンス領域1 4 1 5 Bに格納した後に受信s t a t e 7 3がOFFされる(図10のステップS 1 6 2)。したがって、ステップ1 3 8からステップS 1 6 2までの間、受信s t a t e 7 3は、ONされたままであるので、何らかの原因によって通信が切断されたとき、メモ리카ード1 1 0の受信ログ7 0から受信s t a t e 7 3を読み出し、受信s t a t e 7 3がONかOFFかを調べれば、どの状態で通信が切断されたのかが解かる。つまり、読み出した受信s t a t e 7 3がONであればライセンスがメモ리카ード1 1 0のライセンス領域1 4 1 5 Bに格納されていないときに通信が切断されたことになり、受信s t a t e 7 3がOFFであれば、ライセンスがメモ리카ード1 1 0のライセンス領域1 4 1 5 Bに格納された後に通信が切断されたことになる。

また、メモ리카ード1 2 0からメモ리카ード1 1 0へのライセンスの移動/複製処理においても図14のステップS 3 3 2から図16のステップS 3 6 4までの間、受信s t a t e 7 3がONされたままであるので、この場合にもライセンスの配信の場合と同じことが言える。

#### 25      [復元]

図14～図16に示すフローチャートに従ってライセンスをメモ리카ード1 2 0からメモ리카ード1 1 0へ移動する途中で通信が切断されたときに、メモ리카ード1 2 0において移動の対象となったライセンスを復元する動作を図18および図19を参照して説明する。すなわち、図15のステップS 3 4 8において

「移動」と判断された後、ステップS 3 5 0から図1 6のステップS 3 6 4の間に通信が中断する等の理由によって移動処理が中断した場合、ライセンスが送信側のメモ리카ード1 2 0および受信側のメモ리카ード1 1 0のいずれにも存在しな状態になり、ライセンスの消失が存在する。この場合に、送信側のメモ리카ード1 2 0において移動の対象となったライセンスを復元することにしたものである。この場合も図1 3に示す系を想定する。

図1 8を参照して、携帯電話機1 0 0の操作パネル1 1 0 8から復元リクエストが入力されると（ステップS 4 0 0）、コントローラ4 0は、認証データの送信要求をインタフェース6 0を介してメモ리카ード1 1 0へ送信する（ステップS 4 0 2）。そして、メモ리카ード1 1 0のコントローラ1 4 2 0は、端子1 4 2 6、インタフェース1 4 2 4およびバスB S 4を介して認証データの送信要求を受信する（ステップS 4 0 4）。

コントローラ1 4 2 0は、認証データの送信要求を受信すると、認証データ保持部1 4 0 0から認証データ {K P m 3 / / C m 3} K P aをバスB S 4を介して読出し、その読出した認証データ {K P m 3 / / C m 3} K P aをバスB S 4、インタフェース1 4 2 4および端子1 4 2 6を介してコントローラ4 0へ出力する（ステップS 4 0 6）。そして、コントローラ4 0は、インタフェース6 0を介して認証データ {K P m 3 / / C m 3} K P aを受取り、インタフェース6 0を介してメモ리카ード1 2 0へ認証データ {K P m 3 / / C m 3} K P aを送信する（ステップS 4 0 8）。

そうすると、メモ리카ード1 2 0のコントローラ1 4 2 0は、端子1 4 2 6およびインタフェース1 4 2 4を介して認証データ {K P m 3 / / C m 3} K P aを受信し、その受信した認証データ {K P m 3 / / C m 3} K P aをバスB S 4を介して復号処理部1 4 0 8へ与える。そして、復号処理部1 4 0 8は、K P a保持部1 4 1 4からの公開認証鍵K P aによって認証データ {K P m 3 / / C m 3} K P aの復号処理を実行する（ステップS 4 1 0）。コントローラ1 4 2 0は、復号処理部5 2 0 8における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモ리카ード1 1 0が正規のメモ리카ードであって、メモ리카ード1 1 0から正規の機関でその正当性を証明するための暗号を施した認証デー

タを受信したか否かを判断する認証処理を行なう（ステップS 4 1 2）。正当な認証データであると判断された場合、コントローラ1 4 2 0は、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を承認し、受理する。そして、次の処理（ステップS 4 1 4）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を受理しないで処理を終了する（ステップS 4 6 2）。

認証の結果、正当な認証データを持つメモリカードを備えるメモリカードからの認証データであることが確認されると、メモリカード1 2 0において、コントローラ1 4 2 0は、セッションキー発生部1 4 1 8を制御し、セッションキー発生部1 4 1 8は、移動のためのセッションキーK s 2 cを生成する（ステップS 4 1 4）。セッションキーK s 2 cは、復号処理部1 4 0 8によって得られたメモリカード1 1 0に対応するクラス公開暗号鍵K P m 3によって、暗号処理部1 4 1 0によって暗号化される。そして、コントローラ1 4 2 0は、バスB S 4を介して暗号化データ {K s 2 c} K m 3を取得し、バスB S 4、インタフェース1 4 2 4および端子1 4 2 6を介して暗号化データ {K s 2 c} K m 3を出力する（ステップS 4 1 6）。

コントローラ4 0は、インタフェース6 0を介して暗号化データ {K s 2 c} K m 3を送信側から受理し（ステップS 4 1 8）、その受理した暗号化データ {K s 2 c} K m 3をインタフェース6 0を介してメモリカード1 1 0へ入力する（ステップS 4 2 0）。この入力によってメモリカード1 1 0に対して受信ログの出力を命令することになる。

メモリカード1 1 0のコントローラ1 4 2 0は、端子1 4 2 6、インタフェース1 4 2 4、およびバスB S 4を介して暗号化データ {K s 2 c} K m 3を受理し、暗号化データ {K s 2 c} K m 3を復号処理部1 4 2 2へ与える。復号処理部1 4 2 2は、K m保持部1 4 2 1からの秘密復号鍵K m 3によって暗号化データ {K s 2 c} K m 3を復号してセッションキーK s 2 cを受理する（ステップS 4 2 2）。コントローラ1 4 2 0は、メモリ1 4 1 5のログ領域1 4 1 5 Aの受信ログ7 0からセッションキーK s 2 bを取得し、その取得したセッションキーK s 2 bをスイッチ1 4 4 6の接点P fを介して暗号処理部1 4 0 6に与え

- る。暗号処理部1406は、復号処理部1422によって復号されたセッションキー $K_{s2c}$ をスイッチ1442の接点Paを介して受取り、セッションキー $K_{s2b}$ をセッションキー $K_{s2c}$ によって暗号化して暗号化データ $\{K_{s2b}\} K_{s2c}$ を生成する（ステップS424）。そして、コントローラ1420は、
- 5 受信ログ70からライセンスID、および受信stateを取得し、ライセンスID// $\{K_{s2b}\} K_{s2c}$ //受信stateを生成し、ライセンスID// $\{K_{s2b}\} K_{s2c}$ //受信stateのハッシュ値hashを求める（ステップS426）。つまり、コントローラ1420は、ライセンスID// $\{K_{s2b}\} K_{s2c}$ //受信stateに対する署名を行なう。
- 10 その後、コントローラ1420は、ハッシュ値hashをスイッチ1446の接点Pfを介して暗号処理部1406に与え、暗号処理部1406は、ハッシュ値hashをセッションキー $K_{s2c}$ によって暗号化を行ない、暗号化データ $\{hash\} K_{s2c}$ を生成する（ステップS428）。そして、コントローラ1420は、ライセンスID// $\{K_{s2b}\} K_{s2c}$ //受信state//
- 15  $\{hash\} K_{s2c}$ を生成して出力する（ステップS430）。つまり、ライセンスID// $\{K_{s2b}\} K_{s2c}$ //受信stateに対する署名をさらにセッションキー $K_{s2c}$ によって暗号化することによってライセンスID// $\{K_{s2b}\} K_{s2c}$ //受信stateに対する署名が改竄されるのを防止している。
- 20 コントローラ40は、インタフェース60を介してライセンスID// $\{K_{s2b}\} K_{s2c}$ //受信state// $\{hash\} K_{s2c}$ を受信し、受信stateの確認を行なう（ステップS432）。受信stateがOFFであれば、メモ리카ード120からメモ리카ード110へライセンスが移動/複製された後に通信が切断されたことを意味するので、ライセンスの復元動作は終了する
- 25 （ステップS462）。ステップS432において、受信stateがONであること、つまり、メモ리카ード120からメモ리카ード110へのライセンスの移動/複製の途中で通信が切断されたことが確認されると、コントローラ40は、ライセンスIDの確認を行なう。すなわち、メモ리카ード110から読出したライセンスID（ステップS426）が、メモ리카ード120が保持するライ

センスIDに一致するか否かを確認する。そして、2つのライセンスIDが不一致であるとき、移動／複製の対象となったライセンスを特定できないので、ライセンスの復元動作は終了する（ステップS462）。ステップS434において、2つのライセンスIDが一致すると、コントローラ40は、ライセンスID  
5 // {Ks2b} Ks2c // 受信state // {hash} Ks2cをメモ  
リカード120へ入力する（ステップS436）。

図19を参照して、メモリカード120のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介してライセンスID // {Ks2b} Ks2c // 受信state // {hash} Ks2cを受理し  
10 （ステップS438）、ライセンスID // {Ks2b} Ks2c // 受信stateのハッシュ値hashを求める（ステップS440）。そして、コントローラ1420は、受理した暗号化データ {hash} Ks2cを復号処理部1412へ与え、復号処理部1412は、暗号化データ {hash} Ks2cをセッションキー発生部1418からのセッションキーKs2cによって復号し、メモ  
15 リカード110において生成されたハッシュ値hashを受理する（ステップS442）。

その後、メモリカード120のコントローラ1420は、自ら求めたハッシュ値hash（ステップS440）が、メモリカード110において生成されたハッシュ値hashに一致するか否かの確認を行なう（ステップS444）。そして、2つのハッシュ値hashが不一致であるとき、ライセンスID // {Ks2b} Ks2c // 受信stateに対する署名が改竄されていることになるので、ライセンスの復元処理は終了する（ステップS462）。ステップS444において、2つのハッシュ値hashが一致しているとき、コントローラ1420は、受信stateの確認を行なう（ステップS446）。受信stateが  
25 OFFであれば、メモリカード120からメモリカード110へライセンスが移動／複製された後に通信が切断されたことを意味するので、ライセンスの復元動作は終了する（ステップS462）。ステップS446において、受信stateがONであること、つまり、メモリカード120からメモリカード110へのライセンスの移動／複製の途中で通信が切断されたことが確認されると、コント

ローラ 1 4 2 0 は、受理した暗号化データ {K s 2 b} K s 2 c を復号処理部 1 4 1 2 へ与える。そして、復号処理部 1 4 1 2 は、暗号化データ {K s 2 b} K s 2 c を、セッションキー発生部 1 4 1 8 からのセッションキー K s 2 c によって復号し、セッションキー K s 2 b を受理する（ステップ S 4 4 8）。

- 5      その後、コントローラ 1 4 2 0 は、メモリ 1 4 1 5 のログ領域 1 4 1 5 A の送信ログ 8 0 に記録されたセッションキー K s 2 b を読出し、その読出したセッションキー K s 2 b がメモリカード 1 1 0 から受信したセッションキー K s 2 b に一致するか否かを比較する（ステップ S 4 5 0）。2 つのセッションキーが不一致であるときは、メモリカード 1 1 0 から受信したセッションキー K s 2 b は、
- 10    異なる移動／複製処理を特定するセッションキーであるので、ライセンスの復元処理は終了する（ステップ S 4 6 2）。ステップ S 4 5 0 において、2 つのセッションキーが一致したとき、コントローラ 1 4 2 0 は、メモリ 1 4 1 5 のログ領域 1 4 1 5 A の送信ログにエントリ番号が記録されているか否かを確認し（ステップ S 4 5 2）、エントリ番号が記録されていなければライセンスの移動／複製
- 15    を行なっていなかったことになるので、ライセンスの復元処理は終了する（ステップ S 4 6 2）。ステップ S 4 5 2 において、送信ログにエントリ番号が記録されている場合、コントローラ 1 4 2 0 は、送信ログ内のエントリ番号を読出し、その読出したエントリ番号によって指定された領域に格納されているライセンス ID をライセンス領域 1 4 1 5 B から取得する（ステップ S 4 5 4）。
- 20    そして、コントローラ 1 4 2 0 は、メモリカード 1 1 0 から受信したライセンス ID とメモリカード 1 2 0 のライセンス領域 1 4 1 5 B から取得したライセンス ID とを比較し（ステップ S 4 5 6）、2 つのライセンス ID が不一致であるとき、ライセンスの復元処理は終了する（ステップ S 4 6 2）。ステップ S 4 5 6 において、2 つのライセンス ID が一致したとき、コントローラ 1 4 2 0 は、
- 25    ログ領域 1 4 1 5 A の送信ログに記録されたエントリ番号によって指定されたライセンスの有効フラグを無効から有効にする（ステップ S 4 5 8）。これによって、ライセンスの送信側においてライセンスが復元される。その後、メモリカード 1 2 0 のコントローラ 1 4 2 0 は、ログ領域 1 4 1 5 A の送信ログを初期化し（ステップ S 4 6 0）、ライセンスの復元処理が終了する（ステップ S 4 6

2)。

このように、ライセンスの移動／複製を行っていた相手であること、その行  
なっていた移動／複製処理が特定されること等を条件としてライセンスの復元を  
送信側において行なうことができる。また、ライセンスID／／{Ks2b}K  
5 s2c／／受信stateに対する署名をメモ리카ード110（受信先）とメモ  
リカード120（送信元）とで行ない、両者の署名が一致することを確認してラ  
イセンスの復元処理を続行することによって安全なライセンスの復元を提供する  
ことができる。

10 なお、上記においては、メモ리카ード120からメモ리카ード110へのライ  
センスの移動およびメモ리카ード120からメモ리카ード110へのライセンス  
の移動動作におけるライセンスの復元について説明したが、メモ리카ード110  
からメモ리카ード120へのライセンスの移動および復元についても、図14～  
図16、図18および図19に示すフローチャートに従って行なわれる。また、  
15 メモ리카ード110、120以外の複数のメモ리카ードのいずれかからのライセ  
ンスの移動および復元についても、図14～図16、図18、および図19に示  
すフローチャートに従って行なわれる。

#### [再生]

上述したように、携帯電話機100または再生端末102に装着されたメモリ  
カード110は、配信サーバ10から、直接、暗号化コンテンツデータおよびラ  
20 イセンスを受信できる。また、メモ리카ード110は、パーソナルコンピュータ  
50が配信サーバ10からハード的に取得した暗号化コンテンツデータおよびラ  
イセンスを、「移動」という概念によってパーソナルコンピュータ50から受信  
できる。

25 このように、メモ리카ード110は、各種の方法によって暗号化コンテンツデ  
ータおよびライセンスを受信する。そこで、次に、これらの各種の方法によって  
メモ리카ードが受信した暗号化コンテンツデータの再生について説明する。

図20は、メモ리카ード110が受信したコンテンツデータの再生端末102  
における再生動作を説明するためのフローチャートである。なお、図20におけ  
る処理以前に、再生端末102のユーザは、メモ리카ード110のデータ領域1

4 1 5 Cに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

図20を参照して、再生動作の開始とともに、再生端末100のユーザから操作パネル1108を介して再生リクエストが再生端末100にインプットされる（ステップS700）。そうすると、コントローラ1106は、バスBS3を介して認証データの出力要求をコンテンツ再生回路1550に行ない（ステップS702）、コンテンツ再生回路1550は認証データの出力要求を受信する（ステップS704）。そして、認証データ保持部1500は、認証データ {K P p 1 / / C p 1} K P aを出力し（ステップS706）、コントローラ1106は、メモリカードインタフェース1200を介してメモリカード110へ認証データ {K P p 1 / / C p 1} K P aを入力する（ステップS708）。

そうすると、メモリカード110は、認証データ {K P p 1 / / C p 1} K P aを受信し、復号処理部1408は、受理した認証データ {K P p 1 / / C p 1} K P aを、K P a保持部1414に保持された公開認証鍵K P aによって復号し（ステップS710）、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ {K P p 1 / / C p 1} K P aが正規の認証データであるか否かを判断する認証処理を行なう（ステップS712）。復号できなかった場合、ステップS746へ移行し、再生動作は終了する。認証データを復号できた場合、コントローラ1420は、セッションキー発生部1418を制御し、セッションキー発生部1418は、再生セッション用のセッションキーK s 2を発生させる（ステップS712）。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーK s 2を、復号処理部1408で復号された公開暗号鍵K P p 1によって暗号化した暗号化データ {K s 2} K p 1をバスBS3へ出力する。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ暗号化データ {K s 2} K p 1を出力する（ステップS714）。再生端末102のコントローラ1106は、メモリカードインタフェース1200を介して暗号化データ {K s 2} K p 1を取得する。



そして、コントローラ 1106 は、暗号化データ {K s 2} K p 1 をバス B S 3 を介してコンテンツ再生回路 1550 の復号処理部 1504 へ与え（ステップ S 716）、復号処理部 1504 は、K p 保持部 1502 から出力された、公開暗号鍵 K P p 1 と対になっている秘密復号鍵 K p 1 によって暗号化データ {K s 2} K p 1 を復号し、セッションキー K s 2 を暗号処理部 1506 へ出力する（ステップ S 718）。そうすると、セッションキー発生部 1508 は、再生セッション用のセッションキー K s 3 を発生させ、セッションキー K s 3 を暗号処理部 1506 へ出力する（ステップ S 720）。暗号処理部 1506 は、セッションキー発生部 1508 からのセッションキー K s 3 を復号処理部 1504 からのセッションキー K s 2 によって暗号化して暗号化データ {K s 3} K s 2 を出力し（ステップ S 722）、コントローラ 1106 は、バス B S 3 およびメモ리카ードインタフェース 1200 を介して暗号化データ {K s 3} K s 2 をメモ리카ード 110 へ出力する（ステップ S 724）。

そうすると、メモ리카ード 110 の復号処理部 1412 は、端子 1426、インタフェース 1424、およびバス B S 4 を介して暗号化データ {K s 3} K s 2 を入力する。復号処理部 1412 は、セッションキー発生部 1418 によって発生されたセッションキー K s 2 によって暗号化データ {K s 3} K s 2 を復号して、再生端末 102 で発生されたセッションキー K s 3 を受理する（ステップ S 726）。

再生端末 102 のコントローラ 1106 は、メモ리카ード 110 から事前を取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し（ステップ S 728）、メモ리카ードインタフェース 1200 を介してメモ리카ード 110 へ取得したエントリ番号と再生許諾要求を出力する（ステップ S 730）。

メモ리카ード 110 のコントローラ 1420 は、エントリ番号と再生許諾要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスおよび有効フラグを取得する（ステップ S 732）。そして、コントローラ 1420 は、有効フラグを確認する（ステップ S 733）。ステップ S 733 において、有効フラグが「無」の場合、指定されたエントリにライセンスが存在しないの

で、再生動作が終了する（ステップS 7 4 6）。ステップS 7 3 3において、有効フラグが「有効」の場合、指定されたエントリにライセンスが存在するので次のステップS 7 3 4へ進む。

5       そして、コントローラ1 4 2 0は、アクセス制限情報A C mを確認する（ステップS 7 3 4）。

10       ステップS 7 3 4においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報A C mを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報A C mの再生回数を変更した（ステップS 7 3 6）後に次のステップに進む（ステップS 7 3 8）。一方、アクセス制限情報A C mの再生回数によって再生が制限されていない場合においては、ステップS 7 3 6はスキップされ、アクセス制限情報A C mの再生回数は変更されることなく処理が次のステップ（ステップS 7 3 8）に進行される。

15       ステップS 7 3 4において、当該再生動作において再生が可能であると判断された場合には、メモリ1 4 1 5のライセンス領域1 4 1 5 Bに記録された再生リクエスト曲のライセンス鍵K cおよび再生制御情報A C pがバスB S 4上に出力される（ステップS 7 3 8）。

20       得られたライセンス鍵K cと再生制御情報A C pは、切換スイッチ1 4 4 6の接点P fを介して暗号処理部1 4 0 6に送られる。暗号処理部1 4 0 6は、切換スイッチ1 4 4 2の接点P bを介して復号処理部1 4 1 2より受けたセッションキーK s 3によって切換スイッチ1 4 4 6を介して受けたライセンス鍵K cと再生制御情報A C pとを暗号化し、暗号化データ {K c//A C p} K s 3をバスB S 4に出力する（ステップS 7 3 8）。

25       バスB S 4に出力された暗号化データは、インタフェース1 4 2 4、端子1 4 2 6、およびメモ리카ードインタフェース1 2 0 0を介して再生端末1 0 2に送出される。

再生端末1 0 2においては、メモ리카ードインタフェース1 2 0 0を介してバスB S 3に伝達される暗号化データ {K c//A C p} K s 3を復号処理部1 5

10によって復号処理を行ない、ライセンス鍵K<sub>c</sub>および再生制御情報AC<sub>p</sub>を受理する（ステップS740, S742）。復号処理部1510は、ライセンス鍵K<sub>c</sub>を復号処理部1516に伝達し、再生制御情報AC<sub>p</sub>をバスBS3に出力する。

- 5       コントローラ1106は、バスBS3を介して、再生制御情報AC<sub>p</sub>を受理して再生の可否の確認を行なう（ステップS744）。

ステップS744においては、再生制御情報AC<sub>p</sub>によって再生不可と判断される場合には、再生動作は終了される。

- 10       ステップS744において再生可能と判断された場合、コントローラ1106は、メモ리카ードインタフェース1200を介してメモ리카ード110に暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>を要求する。そうすると、メモ리카ード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>を取得し、バスBS4、インタフェース1424、および端子1426を介してメモ리카ードインタフェース1200へ出力する。

- 15       再生端末102のコントローラ1106は、メモ리카ードインタフェース1200を介して暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>を取得し、バスBS3を介して暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>をコンテンツ再生回路1550へ与える。

- 20       そして、コンテンツ再生回路1550の復号処理部1516は、暗号化コンテンツデータ{D<sub>c</sub>}K<sub>c</sub>を復号処理部1510から出力されたライセンス鍵K<sub>c</sub>によって復号してコンテンツデータD<sub>c</sub>を取得する。

- 25       そして、復号されたコンテンツデータD<sub>c</sub>は音楽再生部1518へ出力され、音楽再生部1518は、コンテンツデータを再生し、DA変換器1519はデジタル信号をアナログ信号に変換して端子1530へ出力する。そして、音楽データは端子1530から外部出力装置を介してヘッドホーン130へ出力されて再生される。これによって再生動作が終了する（ステップS746）。

パーソナルコンピュータ50のライセンス専用メモ리카ード520における暗号化コンテンツデータの再生動作も図20に示すフローチャートに従って行なわれる。

また、パーソナルコンピュータ 50 は、ライセンス専用メモリカード 520 を装着し、その装着したライセンス専用メモリカード 520 にライセンスを記録するものとして説明したが、ライセンス専用メモリカード 520 に代えて、メモリカード 110 を装着し、その装着したメモリカードにライセンスのみを管理させることも可能である。

さらに、メモリカード 110 を携帯電話機 100 またはデータ再生端末 102 に装着した場合と同様に、暗号化コンテンツデータおよびライセンス管理情報をライセンス専用メモリカード 520 のデータ領域 1415C に記録して用いることも可能である。

また、さらに、ライセンス専用メモリカード 520 に代えて、データ領域 1415C を備えないライセンス専用メモリカードやライセンス専用の記録デバイス（半導体チップ）などを用いることも可能である。この場合、エントリ管理情報はハードディスク 530 に記録される。

また、さらに、パーソナルコンピュータ 50 においては、暗号アルゴリズムを備え、ソフトウェアによって耐タンパモジュールを実現したライセンス管理プログラムによってライセンス専用メモリカード 520 の機能を実現することも可能である。この場合、ログ領域 1415A およびライセンス領域 1415B は、ハードディスク 530 に設けられ、ライセンス管理プログラムによって独自に暗号化され、ライセンス管理プログラム以外からアクセスしても、内容が確認および書換えができないように構成される。また、パーソナルコンピュータ 50 のハードディスク 530 またはコントローラ 510 に関連付けて記録され、パーソナルコンピュータ 50 においてのみアクセス可能となるように構成される。さらに、図 14～図 16 に示すフローチャートによらない移動／複製されたライセンスは、無効となるように構成される。

本発明の実施の形態によれば、送信元のメモリカードは、ライセンスの移動を有効フラグによって管理し、ライセンスの移動の途中で通信が切断されたとき、ライセンスの移動を行っていた相手であること等を確認して有効フラグを有効にするので、送信元におけるライセンスの復元を容易に行なうことができる。

上記の説明において、ライセンスを移動させるとき有効フラグを用いることに

より送信側のメモリカードにおいて移動対象となるライセンスを復元でき、かつ、使用不能となる状態を実現した。この他に、たとえば、移動の対象となるライセンスをメモリカードのメモリ 1 4 1 5 のログ領域 1 4 1 5 A の送信ログに 1  
5 ライセンス分の待避ライセンスを格納できるようにログ領域 1 4 1 5 A を拡張し、移動の対象となるライセンスを送信ログに待避して、移動するライセンスが記録されているエントリ内を消去することで実現可能である。この場合、エントリごとに設けられる有効フラグは必要ない。

この構成の場合、移動処理においては、送信側のメモリカード 1 1 0 では図 1  
5 のステップ S 3 5 0 において、指定されたエントリ番号および指定されたエン  
10 トリ番号内のライセンスをログ領域 1 4 1 5 A の送信ログに格納し、指定されたエントリ番号内のライセンスを消去する。受信側のメモリカード 1 2 0 では、ステップ S 3 6 4 を、「ライセンス（ライセンス ID、コンテンツ ID、ライセンス鍵 K c、アクセス制御情報 A C m、および再生制御情報 A C p）をエントリ番号で指定されたエントリに格納する」ように変更すればよい。さらに、復元処理  
15 において、図 1 9 のステップ S 4 5 8 を、「待避ライセンスを送信ログ内のエントリ番号で示されるエントリに複製する」ように変更すればよい。

同様に、配信処理の各処理において、有効フラグの設定および確認を行なう必要がなくなる。この場合、図 1 0 のステップ S 1 6 0 を、「ライセンス（ライセンス ID、コンテンツ ID、ライセンス鍵 K c、アクセス制御情報 A C m、および再生制御情報 A C p）をエントリ番号で指定されたエントリに格納する」よう  
20 に変更する。再生処理では、有効フラグが運用されていないので、図 2 0 のステップ S 7 3 3 の処理は必要なくなる。

上記においては、暗号化コンテンツデータを復号するためのライセンスを例にして、ライセンスの復元処理について説明したが、本発明においては、復元の対象となるものは暗号化コンテンツデータを復号するためのライセンスに限らず、  
25 個人情報、およびクレジットカードの情報等の同時に 2 個以上存在してはいけないデータが復元の対象となる。このようなデータについても、上述した各処理を行なうことができる。

今回開示された実施の形態はすべての点で例示であって制限的なものではない

と考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

5 産業上の利用可能性

本発明によれば、送信元のメモリカードは、ライセンスの移動を有効フラグによって管理し、ライセンスの移動の途中で通信が切断されたとき、ライセンスの移動を行っていた相手であること等を確認して有効フラグを有効にするので、送信元におけるライセンスの復元を容易に行なうことができる。したがって、本

10 発明は、ライセンスの移動中に通信が切断されても、その移動と対象となったライセンスを復元可能なデータ記録装置に適用される。

## 請求の範囲

1. 一義的にのみ存在することが許容される独自データを他のデータ記録装置  
(110, 520)へ移動するデータ記録装置(120)であって、
  - 5 前記他のデータ記録装置(110, 520)への前記独自データの移動処理を  
特定するための第1の履歴情報(81)を保持する履歴情報保持部(1415  
A, 80)と、  
前記独自データを保持する独自データ保持部(1415B)と、  
制御部(1420)とを備え、
    - 10 前記制御部(1420)は、  
前記独自データの前記他のデータ記録装置(110, 520)への移動に対し  
て前記独自データの外部への出力が不可能な状態に変更し、  
前記独自データの復元要求に応じて、前記他のデータ記録装置(110, 52  
0)との通信状態を示す前記他のデータ記録装置(110, 520)に保持され  
15 た通信情報(73)と前記他のデータ記録装置(110, 520)に保持された  
前記移動処理を特定するための第2の履歴情報(72)とを前記他のデータ記録  
装置(110, 520)から受信し、前記通信情報(73)に基づいて前記他の  
データ記録装置(110, 520)との通信状態を確認し、前記通信情報(7  
3)が前記移動の途中を示すとき前記第2の履歴情報(72)が前記第1の履歴  
20 情報(81)に一致するか否かを判定し、前記第2の履歴情報(72)が前記第  
1の履歴情報(81)に一致するとき前記独自データの外部への出力が可能な状  
態に復元する、データ記録装置。  
2. 前記独自データ保持部(1415B)は、前記独自データの一部または全て  
を外部へ出力可能か出力不可かを示す出力可否フラグをさらに保持し、
      - 25 前記制御部(1420)は、  
前記独自データの前記他のデータ記録装置(110, 520)への移動に対し  
て前記出力可否フラグを出力不可に設定し、  
前記独自データの復元時、前記出力可否フラグを出力可能に設定する、請求項  
1に記載のデータ記録装置。

3. 前記履歴情報保持部（1415A, 80）は、前記移動の対象となった独自データを外部へ出力不可能な状態でさらに保持し、

前記制御部（1420）は、

5 前記独自データの前記他のデータ記録装置（110, 520）への移動に対して前記移動の対象となった独自データを前記履歴情報保持部（1415A, 80）に与え、前記独自データ保持部から前記移動の対象となった独自データを消去し、

10 前記独自データの復元時、前記履歴情報保持部（1415A, 80）に保持された独自データを前記独自データ保持部に書込む、請求項1に記載のデータ記録装置。

4. 前記第1の履歴情報（81）は、前記移動のための通信確立時に前記他のデータ記録装置（110, 520）で生成され、かつ、前記他のデータ記録装置（110, 520）から受信された第1のセッション鍵であり、

15 前記第2の履歴情報（72）は、前記移動のための通信確立時に前記他のデータ記録装置（110, 520）で生成され、かつ、前記他のデータ記録装置（110, 520）に保持された前記第1のセッション鍵と同じ第2のセッション鍵である、請求項1から請求項3のいずれか1項に記載のデータ記録装置。

5. 電子署名により前記通信情報（73）と前記第2の履歴情報（72）との正当性を確認する署名確認手段（1420）をさらに備え、

20 前記制御部（1420）は、さらに、前記通信情報（73）と前記第2の履歴情報（72）とに対する電子署名を前記通信情報（73）および前記第2の履歴情報（72）とともに前記他のデータ記録装置（110, 520）から受信し、前記署名確認手段（1420）によって前記通信情報（73）と前記第2の履歴情報（72）の正当性が確認されたとき、前記通信状態を確認し、かつ、前記第  
25 1の履歴情報（81）と前記第2の履歴情報（72）との一致を確認する、請求項1から請求項3のいずれか1項に記載のデータ記録装置。

6. 前記他のデータ記録装置（110, 520）との通信を特定するためのセッション鍵を生成するセッション鍵生成部（1418）と、

前記セッション鍵生成部（1418）が生成したセッション鍵によって暗号化



されたデータを復号する復号部（１４１２）とをさらに備え、

前記独自データの復元時、

前記セッション鍵生成部（１４１８）は、前記独自データの復元のための通信を特定する第３のセッション鍵を生成し、

- ５ 前記制御部（１４２０）は、前記第３のセッション鍵を前記他のデータ記録装置（１１０，５２０）へ送信し、前記第３のセッション鍵によって暗号化された第２の履歴情報（７２）を前記他のデータ記録装置（１１０，５２０）から受信する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

- １０ ７．前記他のデータ記録装置（１１０，５２０）との通信を特定するためのセッション鍵を生成するセッション鍵生成部（１４１８）と、

前記セッション鍵生成部（１４１８）が生成したセッション鍵によって暗号化されたデータを復号する復号部（１４１２）とをさらに備え、

前記独自データの復元時、

- １５ 前記セッション鍵生成部（１４１８）は、前記独自データの復元のための通信を特定する第３のセッション鍵を生成し、

- ２０ 前記制御部（１４２０）は、前記第３のセッション鍵を前記他のデータ記録装置（１１０，５２０）へ送信し、前記第３のセッション鍵によって暗号化された第２の履歴情報（７２）と、前記第３のセッション鍵によって暗号化された前記電子署名のデータとを前記他のデータ記録装置（１１０，５２０）から受信する、請求項５に記載のデータ記録装置。

８．前記履歴情報保持部（１４１５Ａ，８０）は、前記移動の対象となった独自データに含まれる第１のデータ特定情報を前記第１の履歴情報（８１）とともに保持し、

- ２５ 前記制御部（１４２０）は、さらに、前記他のデータ記録装置（１１０，５２０）から受信する前記移動の対象となった前記第２のデータ特定情報が前記第１のデータ特定情報に一致するか否かを判定し、前記第２のデータ特定情報が前記第１のデータ特定情報に一致するとき、前記通信情報（７３）を確認し、かつ、前記第１の履歴情報（８１）と前記第２の履歴情報（７２）との一致を確認する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

9. 電子署名により前記通信情報（73）と前記第2の履歴情報（72）と前記第2のデータ特定情報との正当性を確認する署名確認手段（1420）をさらに備え、

5 前記制御部（1420）は、さらに、前記通信情報（73）と前記第2の履歴情報（72）と前記第2のデータ特定情報とに対する電子署名を、前記通信情報（73）と前記第2の履歴情報（72）と前記第2のデータ特定情報とともに受信し、前記署名確認手段（1420）によって前記通信情報（73）と前記第2の履歴情報（72）と前記第2のデータ特定情報の正当性が確認されたとき、前記第2のデータ特定情報と前記第1のデータ特定情報との一致を確認し、かつ、  
10 前記通信情報（73）を確認し、前記第1の履歴情報（81）と前記第2の履歴情報（72）との一致を確認する、請求項8に記載のデータ記録装置。

10. 前記他のデータ記録装置（110, 520）または前記他のデータ記録装置（110, 520）と異なるもう1つの他のデータ記録装置との通信状態を示すもう1つの通信情報を保持する通信情報保持部（1415A, 70）と、

15 前記他のデータ記録装置（110, 520）または前記もう1つの他のデータ記録装置からの独自データの移動処理を特定するための第3の履歴情報を保持するもう1つの履歴情報保持部（1415A, 70）とをさらに備え、

前記制御部（1420）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（110, 520）または前記もう1つの  
20 他のデータ記録装置から受信するとき、前記第3の履歴情報を前記もう1つの履歴情報保持部（1415A, 70）に記録し、外部からの履歴情報の出力要求に応じて前記通信情報（73）と前記第3の履歴情報とを出力する、請求項1から請求項3のいずれか1項に記載のデータ記録装置。

11. 前記他のデータ記録装置（110, 520）または前記もう1つの他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部（1418）をさらに備え、  
25

前記セッション鍵生成部（1418）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（110, 520）または前記もう1つの他のデータ記録装置から受信するための通信を特定する第4のセ

セッション鍵を生成し、

前記制御部（１４２０）は、前記移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つのデータ記録装置から受信する通信の確立時、前記第４のセッション鍵を前記他のデータ記録装置（１１０，５  
5 ２０）または前記もう１つのデータ記録装置へ送信するとともに前記第４のセッション鍵を前記第３の履歴情報として前記もう１つの履歴情報保持部（１４１５Ａ，７０）に格納し、外部からの履歴情報の出力要求に応じて前記もう１つの通信情報および前記第３の履歴情報を出力する、請求項１０に記載のデータ記録装置。

10 １２．前記もう１つの通信情報と前記第３の履歴情報とに対する電子署名を生成する電子署名生成部（１４２０）をさらに備え、

前記制御部（１４２０）は、外部からの履歴情報の出力要求に応じて、前記もう１つの通信情報と前記第３の履歴情報と前記電子署名とを出力する、請求項１１に記載のデータ記録装置。

15 １３．前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から入力された第５のセッション鍵によって暗号化する暗号処理部（１４０６）をさらに備え、

前記制御部（１４２０）は、前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から前記独自データを受信する通信の確立  
20 時、前記第４のセッション鍵を前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置に出力するとともに前記第４のセッション鍵を前記第３の履歴情報として前記もう１つの履歴情報保持部（１４１５Ａ，７０）に格納し、外部からの履歴情報の出力要求に応じて前記もう１つの通信情報と前記暗号処理部（１４０６）において前記第５のセッション鍵によって暗号化された前記第３の履歴情報とを出力する、請求項１１に記載のデータ記録装置。  
25

１４．前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から入力された第５のセッション鍵によってデータを暗号化する暗号処理部（１４０６）と、

前記通信情報（７３）と前記暗号処理部（１４０６）において外部から入力さ

れた第3のセッション鍵によって暗号化された第3の履歴情報とに対する電子署名を生成する電子署名生成部（1420）とをさらに備え、

前記暗号処理部（1406）は、前記第5のセッション鍵によって前記第3の履歴情報と前記電子署名とを暗号化し、

- 5 前記制御部（1420）は、前記他のデータ記録装置（110, 520）または前記もう1つの他のデータ記録装置から前記独自データを受信する通信の確立時、前記第4のセッション鍵を前記他のデータ記録装置（110, 520）または前記もう1つの他のデータ記録装置に出力するとともに前記第4のセッション鍵を前記第3の履歴情報として前記もう1つの履歴情報保持部（1415A, 70）に格納し、外部からの履歴情報の出力要求に応じて、前記通信情報（73）と前記第5のセッション鍵によって暗号化された前記第3の履歴情報と前記第5のセッション鍵によって暗号化された前記電子署名とを出力する、請求項11に記載のデータ記録装置。
- 10

- 15 15. 前記制御部（1420）は、前記他のデータ記録装置（110, 520）または前記もう1つの他のデータ記録装置からの移動の対象となる独自データを特定する第3のデータ特定情報を前記通信情報保持部（1415A, 70）に記録し、前記第3のデータ特定情報の出力要求に応じて、前記通信情報保持部（1415A, 70）から前記第3のデータ特定情報を読出して前記通信情報（73）および前記第3の履歴情報とともに出力する、請求項10に記載のデータ記録装置。
- 20

16. 前記独自データは、暗号化コンテンツデータを復号するためのライセンスである、請求項1から請求項3のいずれか1項に記載のデータ記録装置。

## 補正書の請求の範囲

[2002年7月3日(03.07.02)国際事務局受理：出願当初の請求の範囲  
5、8、9及び10-16は補正された；新しい請求の範囲17が加えられた；  
他の請求の範囲は変更なし。(8頁)]

3. 前記履歴情報保持部(1415A, 80)は、前記移動の対象となった独自データを外部へ出力不可能な状態でさらに保持し、

前記制御部(1420)は、

5 前記独自データの前記他のデータ記録装置(110, 520)への移動に対して前記移動の対象となった独自データを前記履歴情報保持部(1415A, 80)に与え、前記独自データ保持部から前記移動の対象となった独自データを消去し、

10 前記独自データの復元時、前記履歴情報保持部(1415A, 80)に保持された独自データを前記独自データ保持部に書込む、請求項1に記載のデータ記録装置。

4. 前記第1の履歴情報(81)は、前記移動のための通信確立時に前記他のデータ記録装置(110, 520)で生成され、かつ、前記他のデータ記録装置(110, 520)から受信された第1のセッション鍵であり、

15 前記第2の履歴情報(72)は、前記移動のための通信確立時に前記他のデータ記録装置(110, 520)で生成され、かつ、前記他のデータ記録装置(110, 520)に保持された前記第1のセッション鍵と同じ第2のセッション鍵である、請求項1から請求項3のいずれか1項に記載のデータ記録装置。

5. (補正後)電子署名により前記通信情報(73)と前記第2の履歴情報(72)との正当性を確認する署名確認部(1420)をさらに備え、

20 前記制御部(1420)は、さらに、前記通信情報(73)と前記第2の履歴情報(72)とに対する電子署名を前記通信情報(73)および前記第2の履歴情報(72)とともに前記他のデータ記録装置(110, 520)から受信し、前記署名確認部(1420)によって前記通信情報(73)と前記第2の履歴情報(72)の正当性が確認されたとき、前記通信状態を確認し、かつ、前記第1  
25 の履歴情報(81)と前記第2の履歴情報(72)との一致を確認する、請求項1から請求項3のいずれか1項に記載のデータ記録装置。

6. 前記他のデータ記録装置(110, 520)との通信を特定するためのセッション鍵を生成するセッション鍵生成部(1418)と、

前記セッション鍵生成部(1418)が生成したセッション鍵によって暗号化

されたデータを復号する復号部（１４１２）とをさらに備え、

前記独自データの復元時、

前記セッション鍵生成部（１４１８）は、前記独自データの復元のための通信を特定する第３のセッション鍵を生成し、

- 5 前記制御部（１４２０）は、前記第３のセッション鍵を前記他のデータ記録装置（１１０，５２０）へ送信し、前記第３のセッション鍵によって暗号化された第２の履歴情報（７２）を前記他のデータ記録装置（１１０，５２０）から受信する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

7. 前記他のデータ記録装置（１１０，５２０）との通信を特定するためのセッション鍵を生成するセッション鍵生成部（１４１８）と、

前記セッション鍵生成部（１４１８）が生成したセッション鍵によって暗号化されたデータを復号する復号部（１４１２）とをさらに備え、

前記独自データの復元時、

- 15 前記セッション鍵生成部（１４１８）は、前記独自データの復元のための通信を特定する第３のセッション鍵を生成し、

- 前記制御部（１４２０）は、前記第３のセッション鍵を前記他のデータ記録装置（１１０，５２０）へ送信し、前記第３のセッション鍵によって暗号化された第２の履歴情報（７２）と、前記第３のセッション鍵によって暗号化された前記電子署名のデータとを前記他のデータ記録装置（１１０，５２０）から受信する、請求項５に記載のデータ記録装置。

8. （補正後）前記履歴情報保持部（１４１５Ａ，８０）は、前記移動の対象となった独自データに含まれる第１のデータ特定情報を前記第１の履歴情報（８１）とともに保持し、

- 25 前記制御部（１４２０）は、さらに、前記他のデータ記録装置（１１０，５２０）から受信する前記移動の対象となった第２のデータ特定情報が前記第１のデータ特定情報に一致するか否かを判定し、前記第２のデータ特定情報が前記第１のデータ特定情報に一致するとき、前記通信情報（７３）を確認し、かつ、前記第１の履歴情報（８１）と前記第２の履歴情報（７２）との一致を確認する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

9. (補正後) 電子署名により前記通信情報(73)と前記第2の履歴情報(72)と前記第2のデータ特定情報との正当性を確認する署名確認部(1420)をさらに備え、

5 前記制御部(1420)は、さらに、前記通信情報(73)と前記第2の履歴情報(72)と前記第2のデータ特定情報とに対する電子署名を、前記通信情報(73)と前記第2の履歴情報(72)と前記第2のデータ特定情報とともに受信し、前記署名確認部(1420)によって前記通信情報(73)と前記第2の履歴情報(72)と前記第2のデータ特定情報の正当性が確認されたとき、前記第2のデータ特定情報と前記第1のデータ特定情報との一致を確認し、かつ、前記通信情報(73)を確認し、前記第1の履歴情報(81)と前記第2の履歴情報(72)との一致を確認する、請求項8に記載のデータ記録装置。

10 10. (補正後) 前記他のデータ記録装置(110, 520)または前記他のデータ記録装置(110, 520)と異なるもう1つの他のデータ記録装置との通信状態を示すもう1つの通信情報(73)を保持する通信情報保持部(1415A, 70)と、

前記他のデータ記録装置(110, 520)または前記もう1つの他のデータ記録装置からの独自データの移動処理を特定するための第3の履歴情報を保持するもう1つの履歴情報保持部(1415A, 70)とをさらに備え、

20 前記制御部(1420)は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置(110, 520)または前記もう1つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部(1415A, 70)に保持されるもう1つの通信情報を更新し、前記第3の履歴情報を前記もう1つの履歴情報保持部(1415A, 70)に記録し、外部からの履歴情報の出力要求に応じて前記もう1つの通信情報(73)と前記第3の履歴情報とを出力する、請求項1から請求項3のいずれか1項に記載のデータ記録装置。

25 11. (補正後) 前記他のデータ記録装置(110, 520)または前記他のデータ記録装置(110, 520)と異なるもう1つの他のデータ記録装置との通信状態を示すもう1つの通信情報(73)を保持する通信情報保持部(1415

A, 70) と、

前記他のデータ記録装置(110, 520)または前記もう1つの他のデータ記録装置からの独自データの移動処理を特定するための第3の履歴情報を保持するもう1つの履歴情報保持部(1415A, 70) と、

- 5 前記他のデータ記録装置(110, 520)または前記もう1つの他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部(1418)をさらに備え、

前記移動対象となる独自データを前記他のデータ記録装置(110, 520)または前記もう1つのデータ記録装置から受信する通信の確立時、

- 10 前記セッション鍵生成部(1418)は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置(110, 520)または前記もう1つの他のデータ記録装置から受信するための通信を特定する第4のセッション鍵を生成し、

- 15 前記制御部(1420)は、前記第4のセッション鍵を前記他のデータ記録装置(110, 520)または前記もう1つのデータ記録装置へ送信するとともに前記第4のセッション鍵を前記第3の履歴情報として前記もう1つの履歴情報保持部(1415A, 70)に格納し、受信する通信の進行と共に前記通信情報保持部(1415A, 70)に保持されるもう1つの通信情報を更新し、外部からの履歴情報の出力要求に応じて前記もう1つの通信情報(73)および前記第3  
20 の履歴情報を出力する、請求項4に記載のデータ記録装置。

12. (補正後) 前記他のデータ記録装置(110, 520)または前記他のデータ記録装置(110, 520)と異なるもう1つの他のデータ記録装置との通信状態を示すもう1つの通信情報(73)を保持する通信情報保持部(1415A, 70) と、

- 25 前記他のデータ記録装置(110, 520)または前記もう1つの他のデータ記録装置からの独自データの移動処理を特定するための第3の履歴情報を保持するもう1つの履歴情報保持部(1415A, 70) と、

前記もう1つの通信情報と前記第3の履歴情報とに対する電子署名を生成する電子署名生成部(1420)をさらに備え、



前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報を前記もう１つの履歴情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて、前記もう１つの通信情報と前記第３の履歴情報と前記電子署名とを出力する、請求項５に記載のデータ記録装置。

１３．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）を保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から入力された第４のセッション鍵によって暗号化する暗号処理部（１４０６）をさらに備え、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報を前記もう１つの履歴情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて前記もう１つの通信情報と前記暗号処理部（１４０６）において前記第４のセッション鍵によって暗号化された前記第３の履歴情報とを出力する、請求項６に記載のデータ記録装置。

１４．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）を保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）と、

5 前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から入力された第４のセッション鍵によってデータを暗号化する暗号処理部（１４０６）と、

前記もう１つの通信情報（７３）と前記暗号処理部（１４０６）において外部から入力された第４のセッション鍵によって暗号化された第３の履歴情報とに対する電子署名を生成する電子署名生成部（１４２０）とをさらに備え、

10 前記暗号処理部（１４０６）は、前記第４のセッション鍵によって前記第３の履歴情報と前記電子署名とを個々に暗号化し、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報を前記もう１つの履歴情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて、前記もう１つの通信情報（７３）と前記第４のセッション鍵によって暗号化された前記第３の履歴情報と前記第４のセッション鍵によって暗号化された前記電子署名とを出力する、請求項７に記載のデータ記録装置。

20 15．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）と前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの移動の対象となる独自データを特定する第３のデータ特定情報とを保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）と、

前記もう 1 つの通信情報と前記第 3 の履歴情報と前記第 3 のデータ特定情報とに対する電子署名を生成する電子署名生成部 (1 4 2 0) とをさらに備え、

前記制御部 (1 4 2 0) は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置 (1 1 0, 5 2 0) または前記もう 1 つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部 (1 4 1 5 A, 7 0) に保持されるもう 1 つの通信情報を更新し、前記第 3 の履歴情報と前記第 3 のデータ特定情報とを前記通信情報部 (1 4 1 5 A, 7 0) に記録し、外部からの履歴情報の出力要求に応じて、前記通信情報保持部 (1 4 1 5 A, 7 0) に記録された前記第 3 のデータ特定情報と前記もう 1 つの通信情報 (7 3) および前記もう 1 つの履歴情報保持部 (1 4 1 5 A, 7 0) に保持された前記第 3 の履歴情報と、前記電子署名生成部によって生成された電子署名とを出力する、請求項 8 に記載のデータ記録装置。

1 6. (補正後) 前記他のデータ記録装置 (1 1 0, 5 2 0) または前記他のデータ記録装置 (1 1 0, 5 2 0) と異なるもう 1 つの他のデータ記録装置との通信状態を示すもう 1 つの通信情報 (7 3) と前記他のデータ記録装置 (1 1 0, 5 2 0) または前記もう 1 つの他のデータ記録装置からの移動の対象となる独自データを特定する第 3 のデータ特定情報とを保持する通信情報保持部 (1 4 1 5 A, 7 0) と、

前記他のデータ記録装置 (1 1 0, 5 2 0) または前記もう 1 つの他のデータ記録装置からの独自データの移動処理を特定するための第 3 の履歴情報を保持するもう 1 つの履歴情報保持部 (1 4 1 5 A, 7 0) とをさらに備え、

前記制御部 (1 4 2 0) は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置 (1 1 0, 5 2 0) または前記もう 1 つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部 (1 4 1 5 A, 7 0) に保持されるもう 1 つの通信情報を更新し、前記第 3 の履歴情報と前記第 3 のデータ特定情報とを前記通信情報保持部 (1 4 1 5 A, 7 0) に記録し、外部からの履歴情報の出力要求に応じて、前記通信情報保持部 (1 4 1 5 A, 7 0) に記録されている前記第 3 のデータ特定情報と前記もう 1 つの通信情報 (7 3) および前記もう 1 つの履歴情報保持部 (1 4 1 5 A,

70) に保持された前記第3の履歴情報とを出力する、請求項9に記載のデータ記録装置。

17. (追加) 前記暗号化コンテンツデータを記憶する記憶部をさらに備え、  
前記独自データは、暗号化コンテンツデータを復号するためのライセンスである、請求項1から請求項3のいずれか1項に記載のデータ記録装置。
- 5

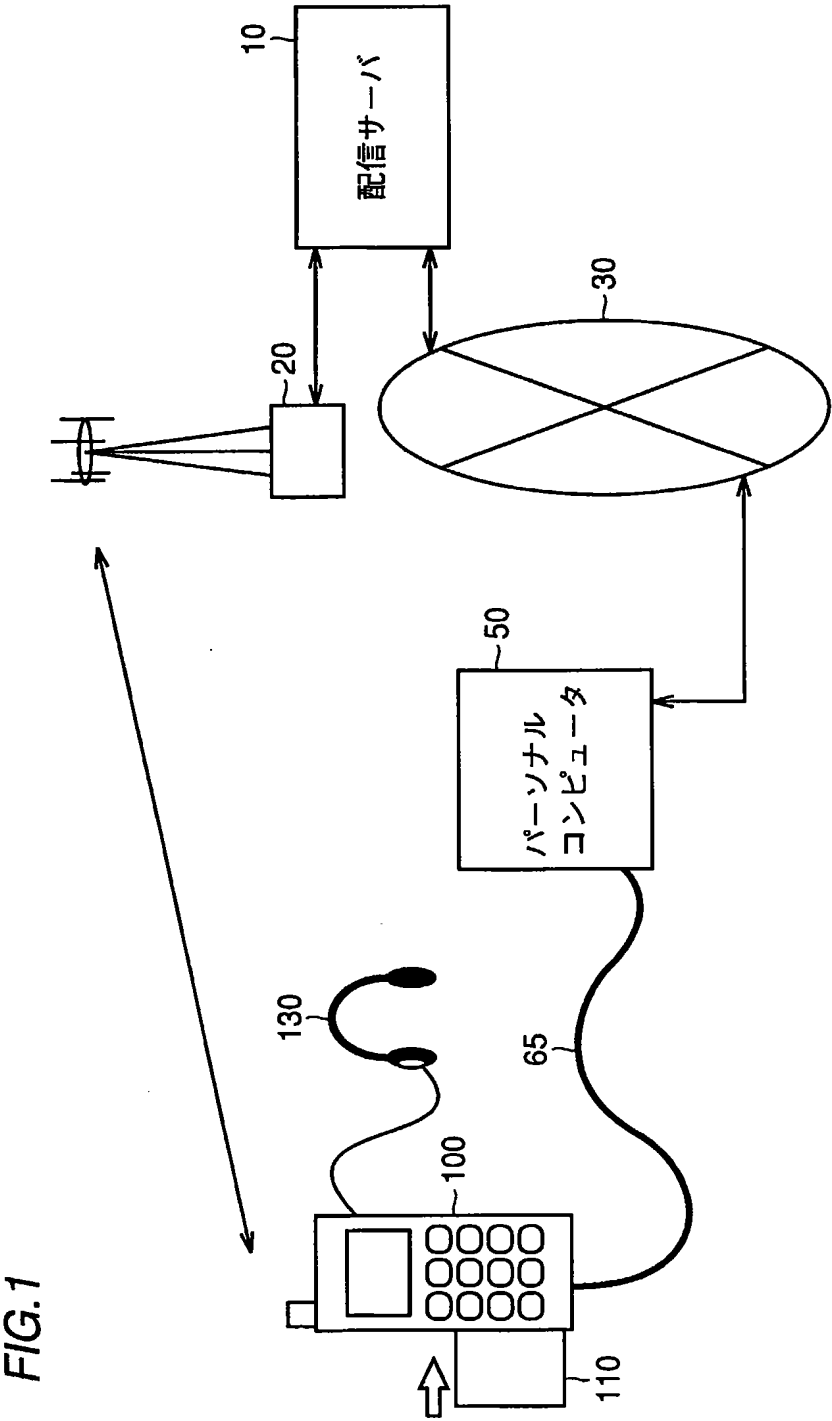


FIG.2

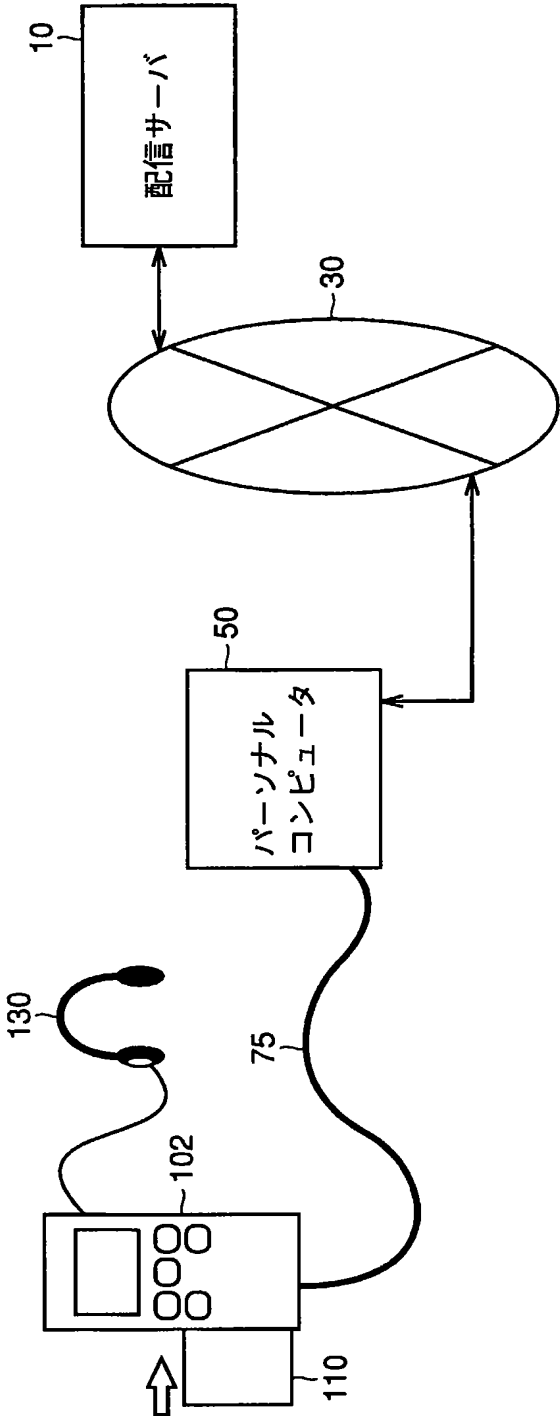


FIG.3

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+コンテンツID+ライセンスIDの総称
有効フラグ	フラグ	ライセンス固有	ライセンスをメモリカードから外部へ出すことが 可能か否かを表す。

FIG.4

記号	種類	属性	特性
KPa/KPb	公開認証鍵	システム 共通	認証局にて認証データを復号する鍵 KPaはレベル1、KPbはレベル2
Ks1	共通鍵	セッション 固有	メモリカード、ライセンス専用メモリカードへのライセンシス配信 ごとに発生
KPa	公開認証鍵	システム 共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な 復号鍵
KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な 復号鍵
Ks2	共通鍵	セッション 固有	配信サーバまたは音楽再生モジュール間のライセンシスの授受ごとに 発生
Cmw	証明書	クラス 証明書	メモリカード、ライセンス専用メモリカードのクラス証明書。 認証機能を有する。 {KPmw/Cmw}KPaの形式で出荷時に記録。 *メモリカード、ライセンス管理デバイス、およびライセンシス管理 モジュールのクラスwごとに異なる。
KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
Ks3	共通鍵	セッション 固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに 発生
Cpy	証明書	クラス 証明書	コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPpy/Cpy}KPaの形式で出荷時に記録。 *コンテンツ再生回路のクラスyごとに異なる。



FIG.5

10

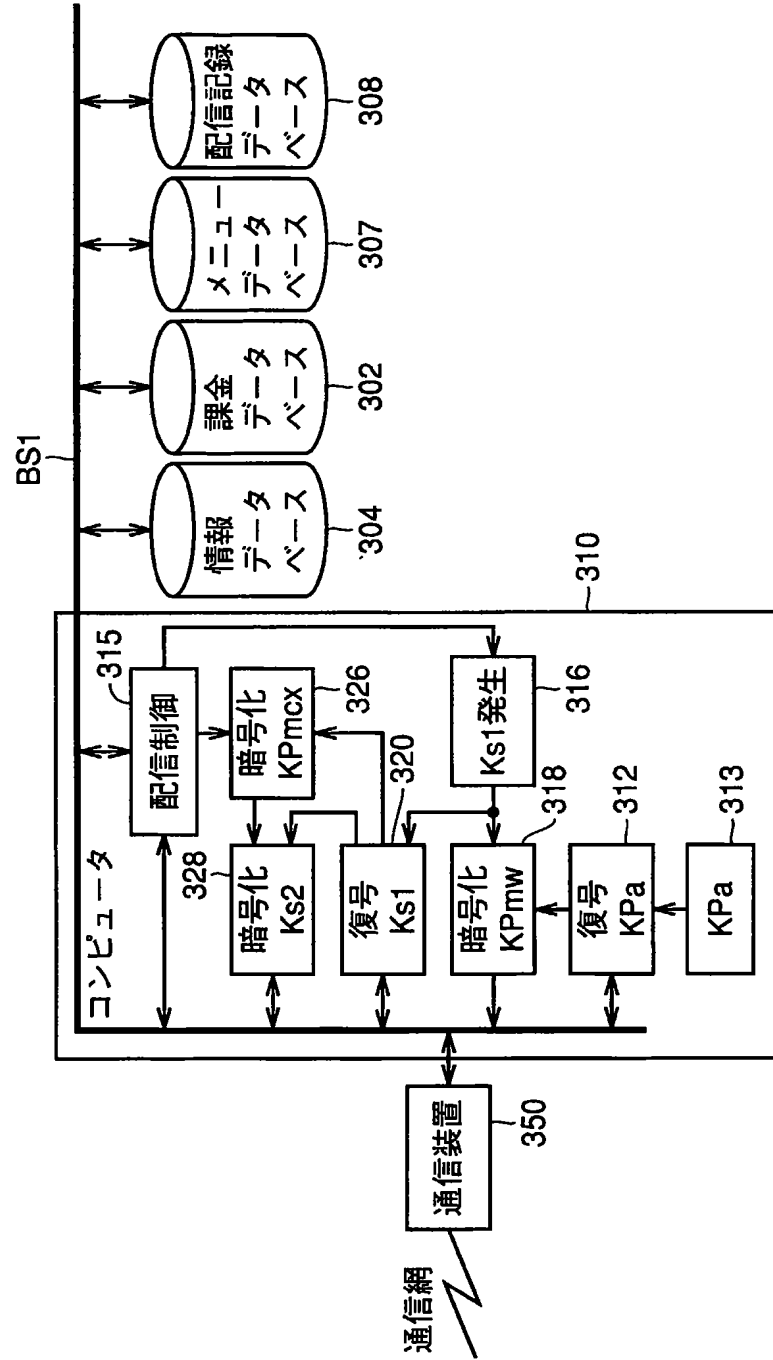


FIG.6

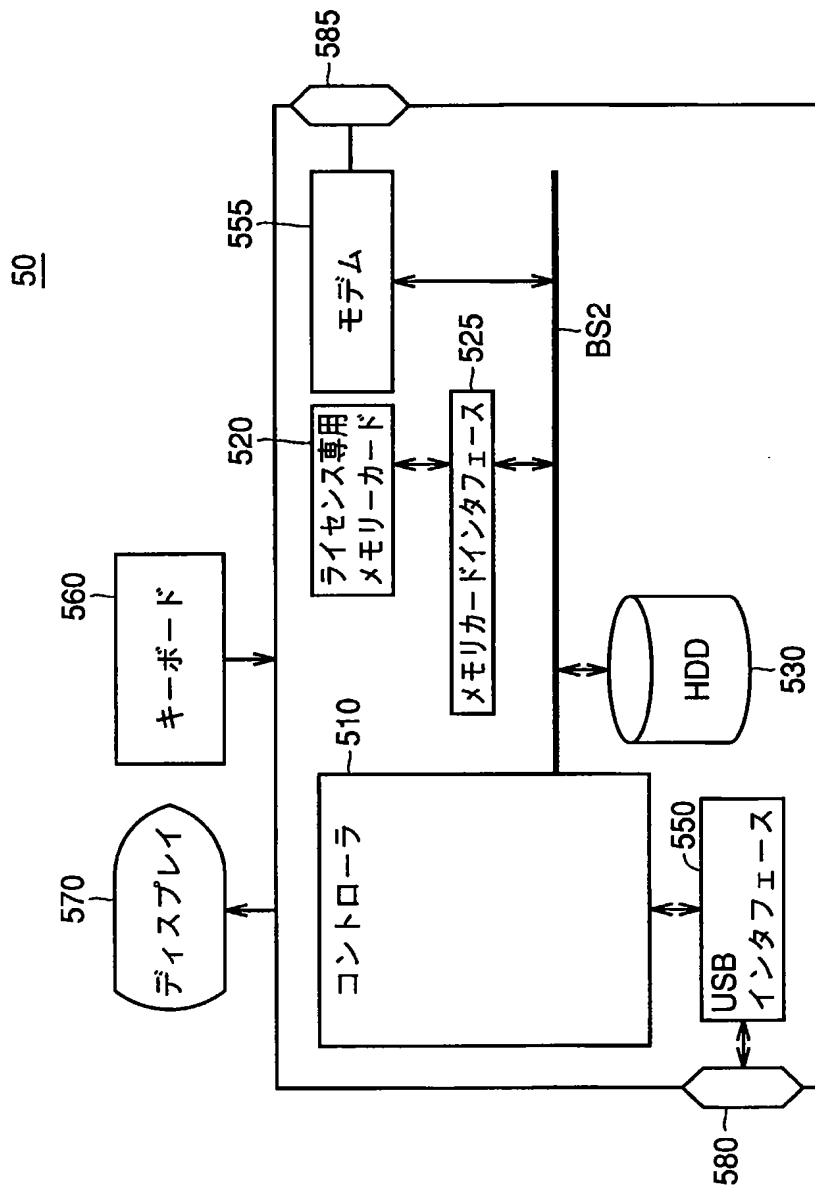
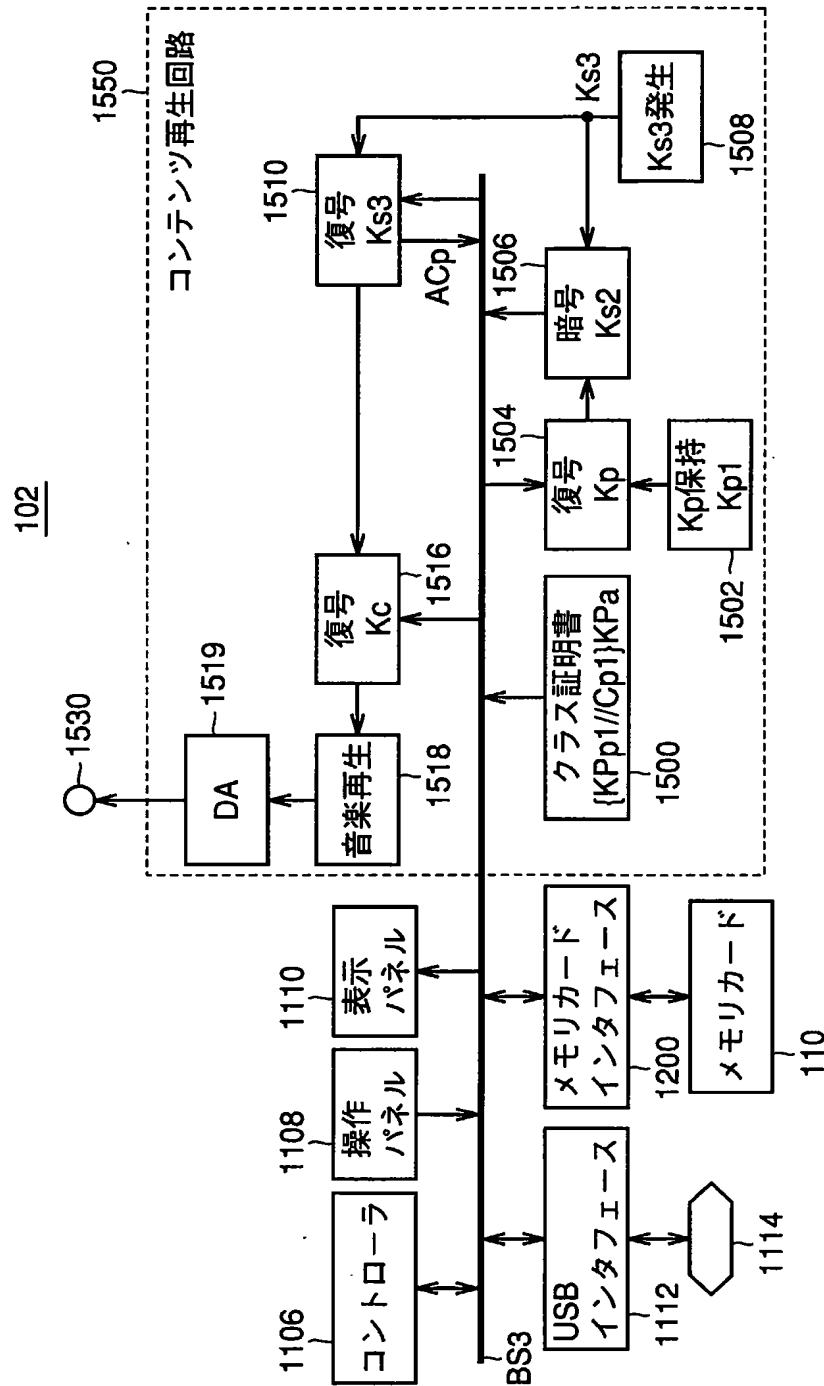


FIG. 7



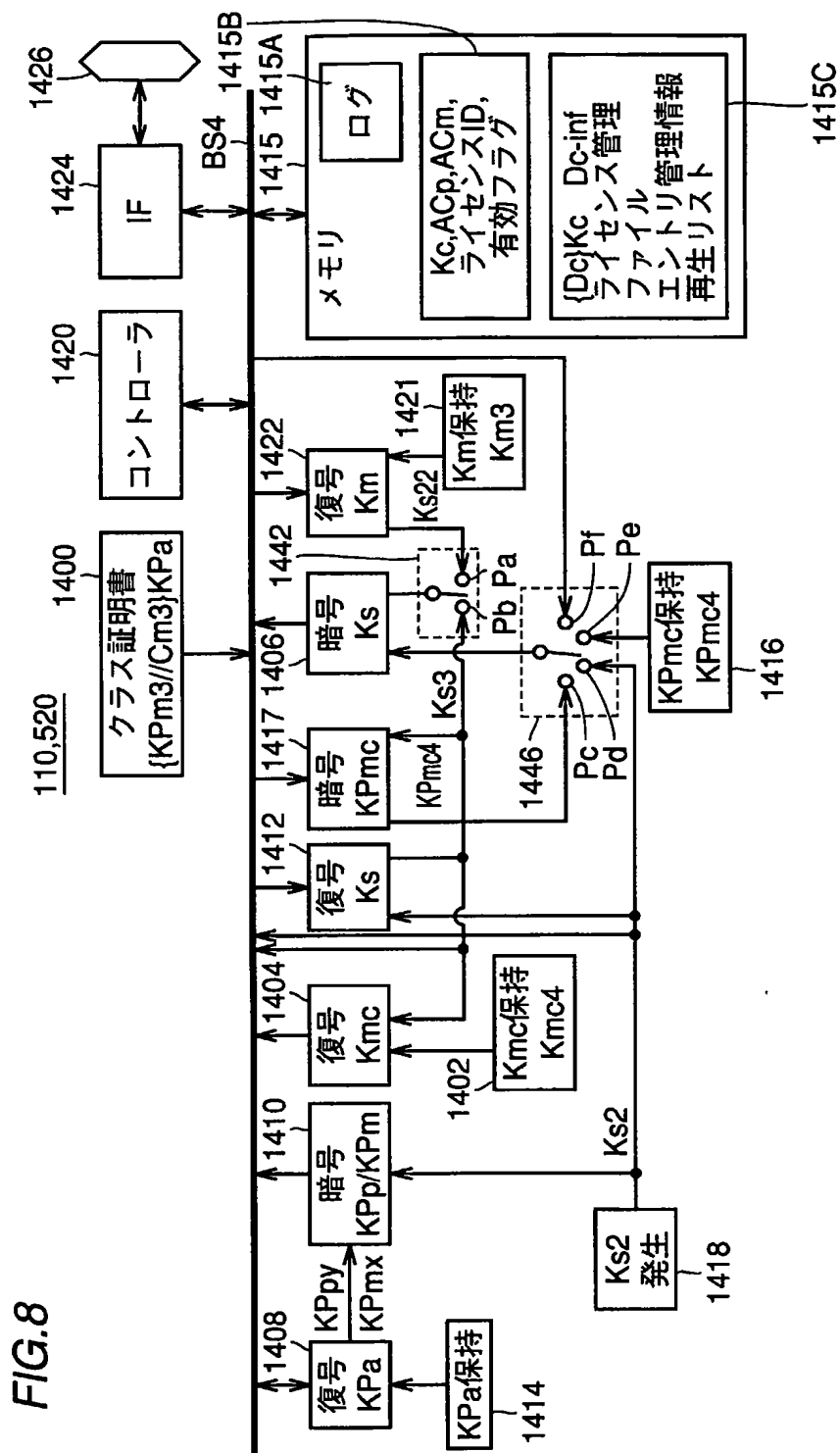


FIG. 9

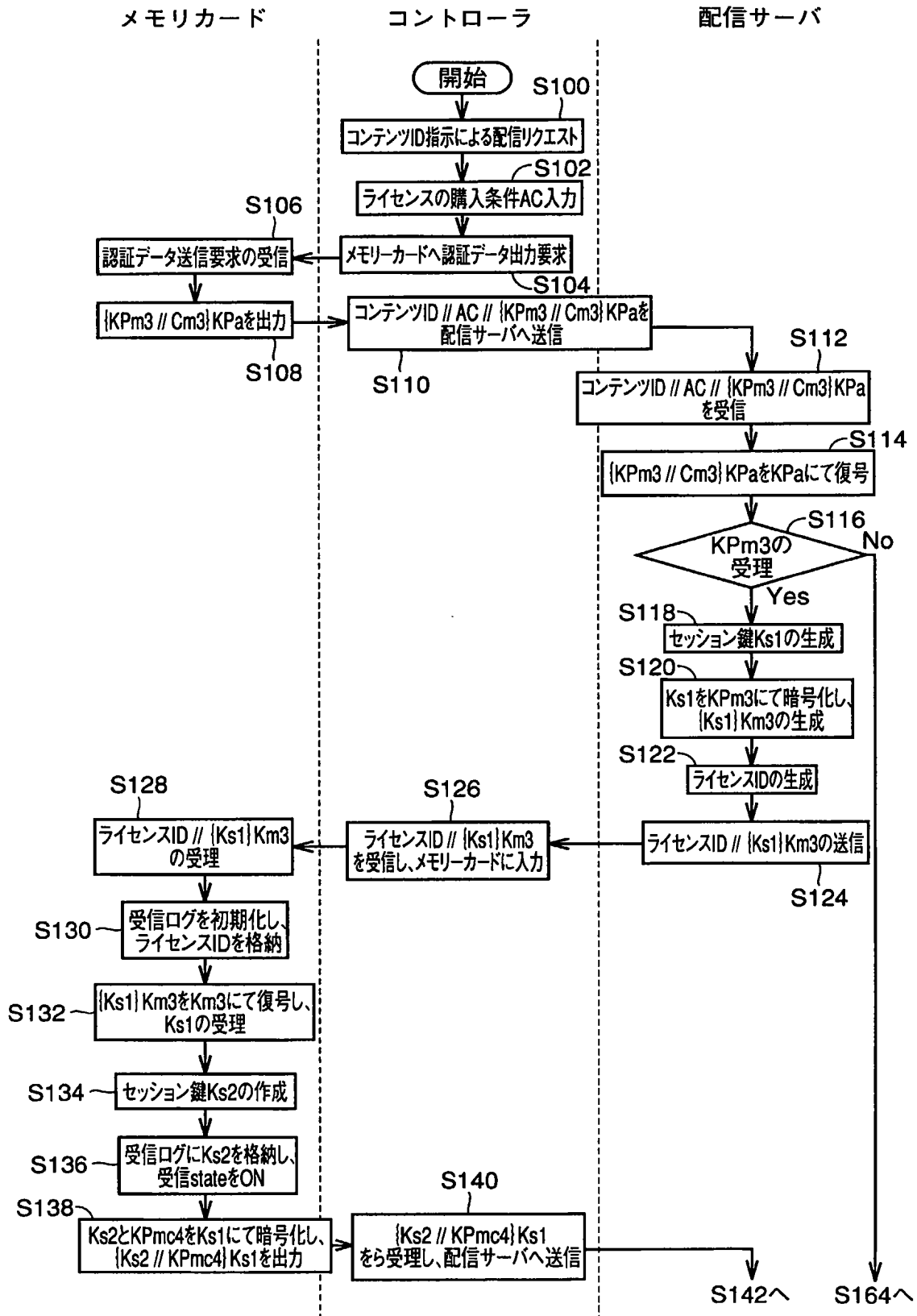
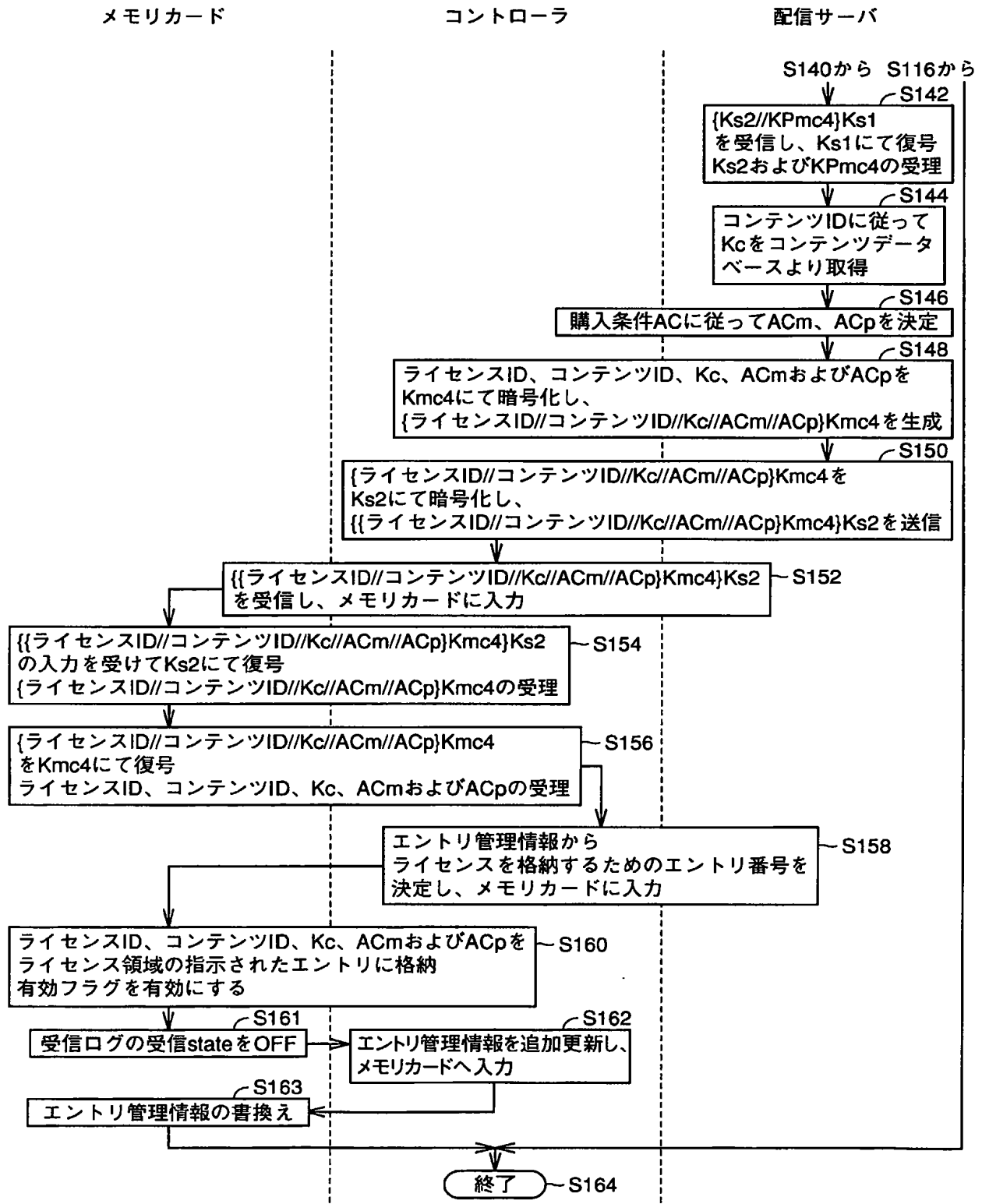


FIG. 10



**FIG. 11**

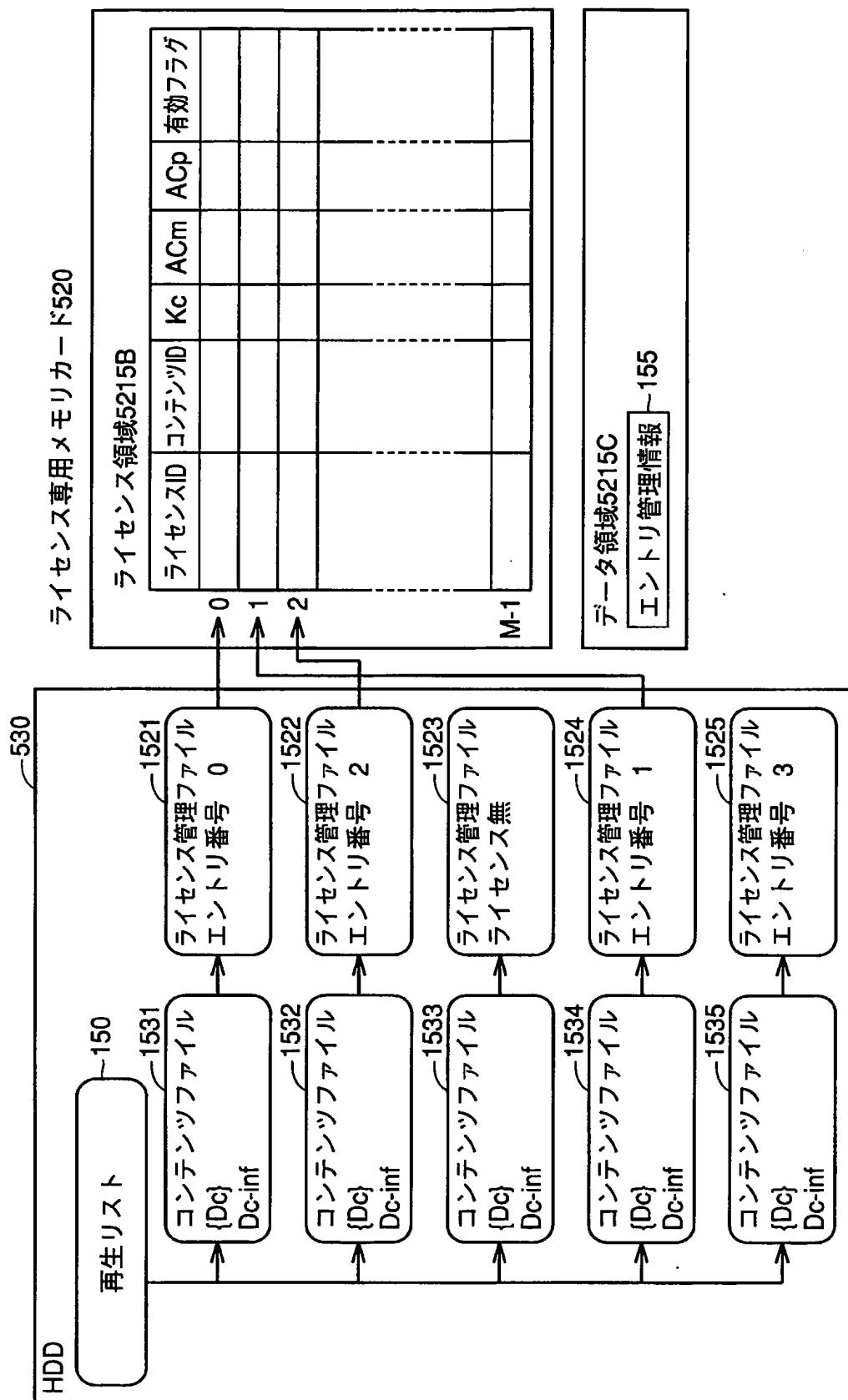


FIG.12

メモリカード110

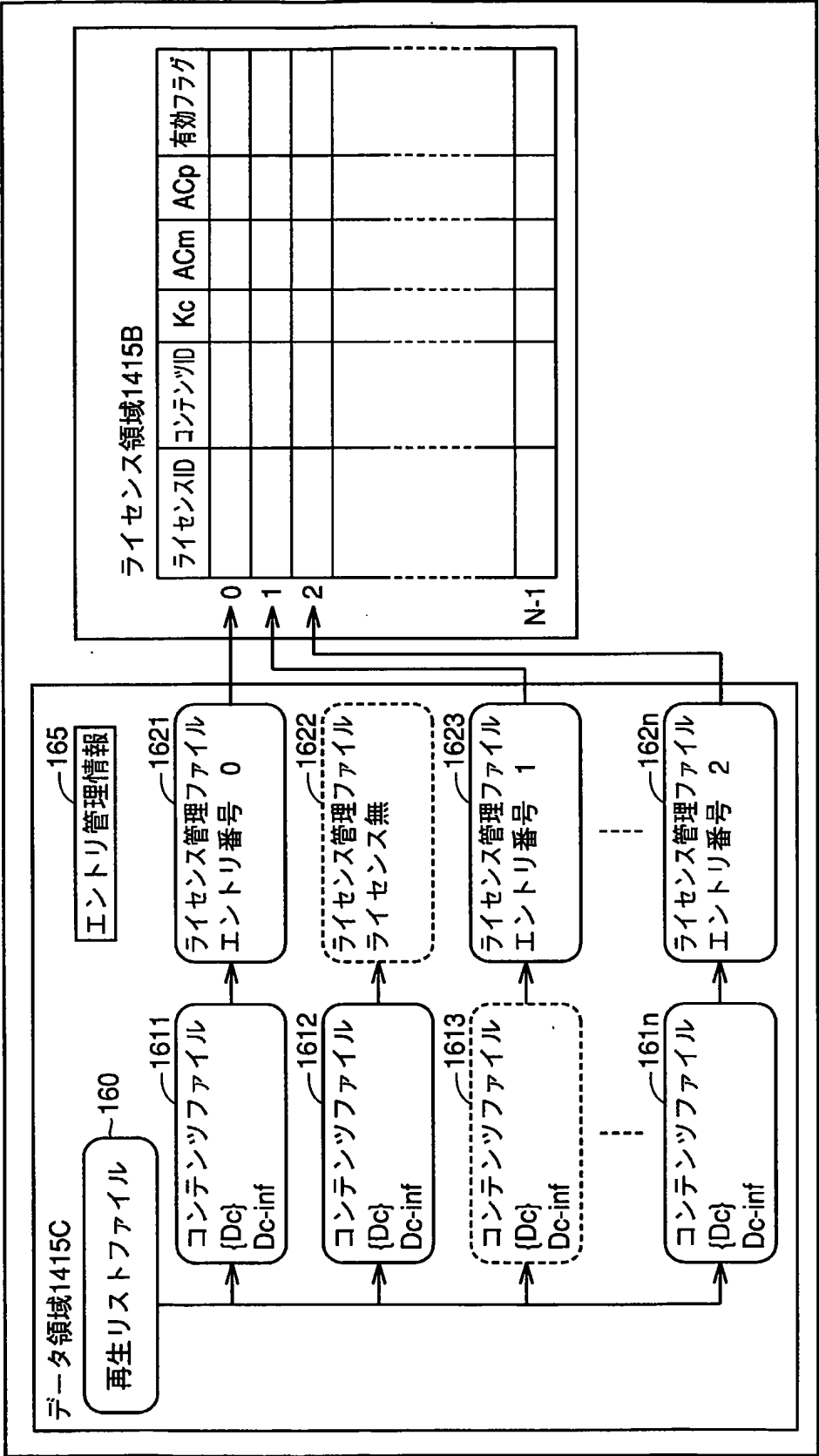




FIG.13

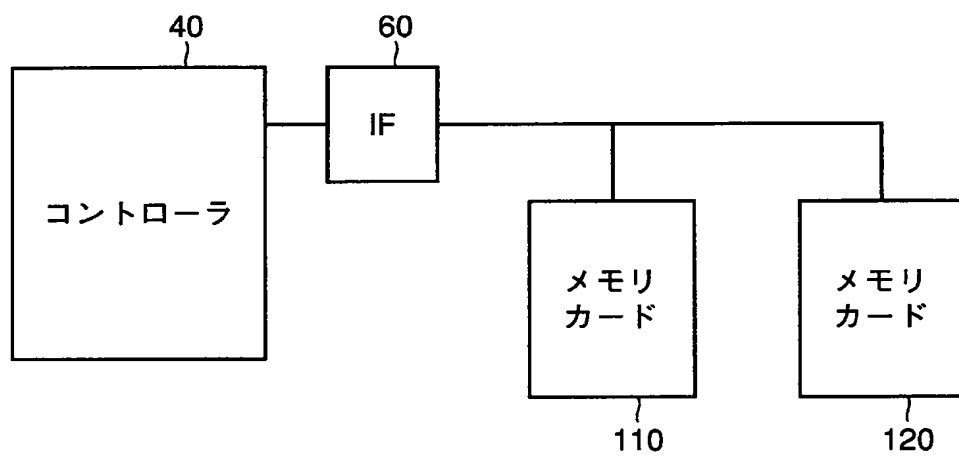


FIG. 14

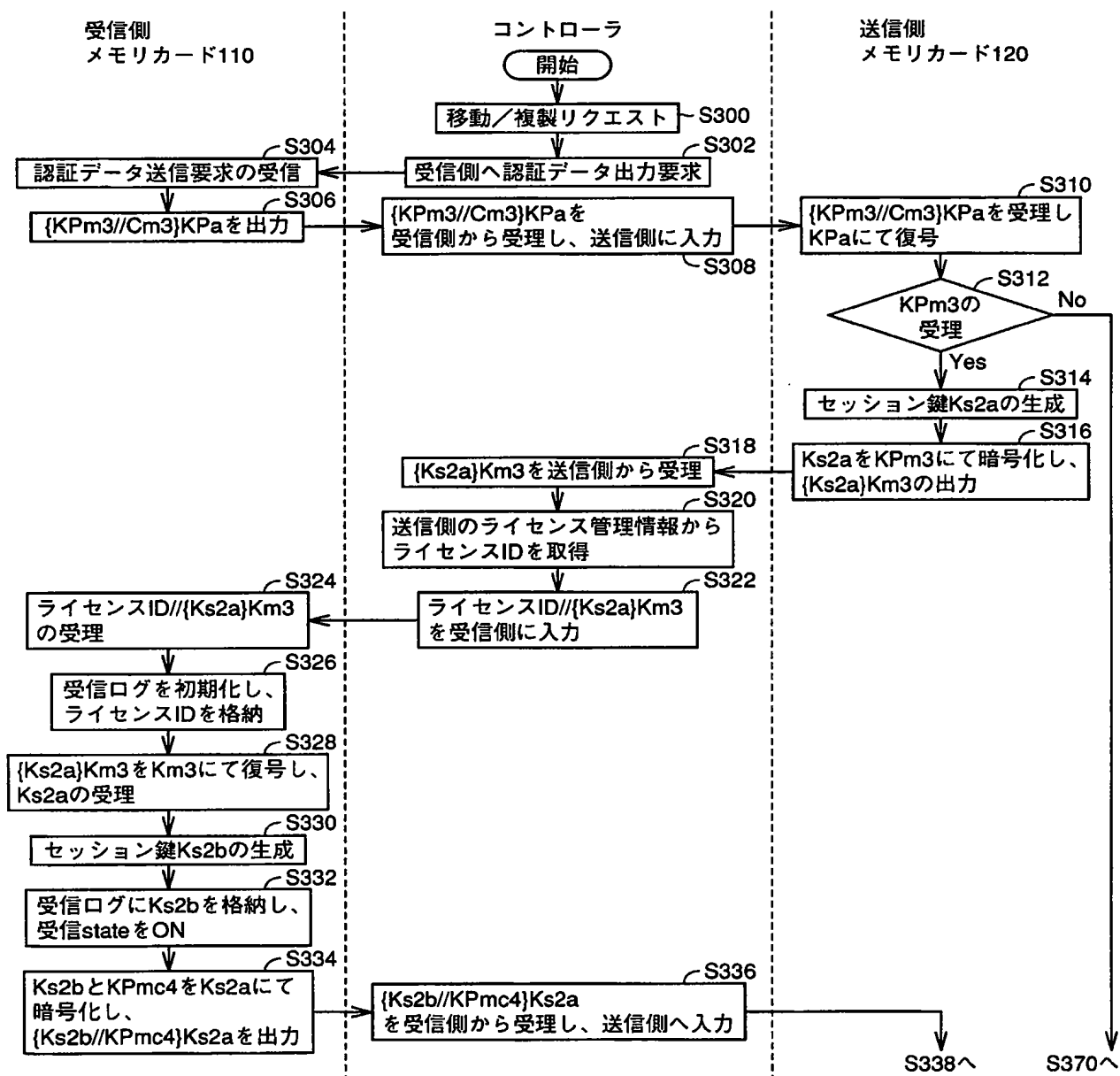


FIG. 15

受信側  
メモリカード110

コントローラ

送信側  
メモリカード120

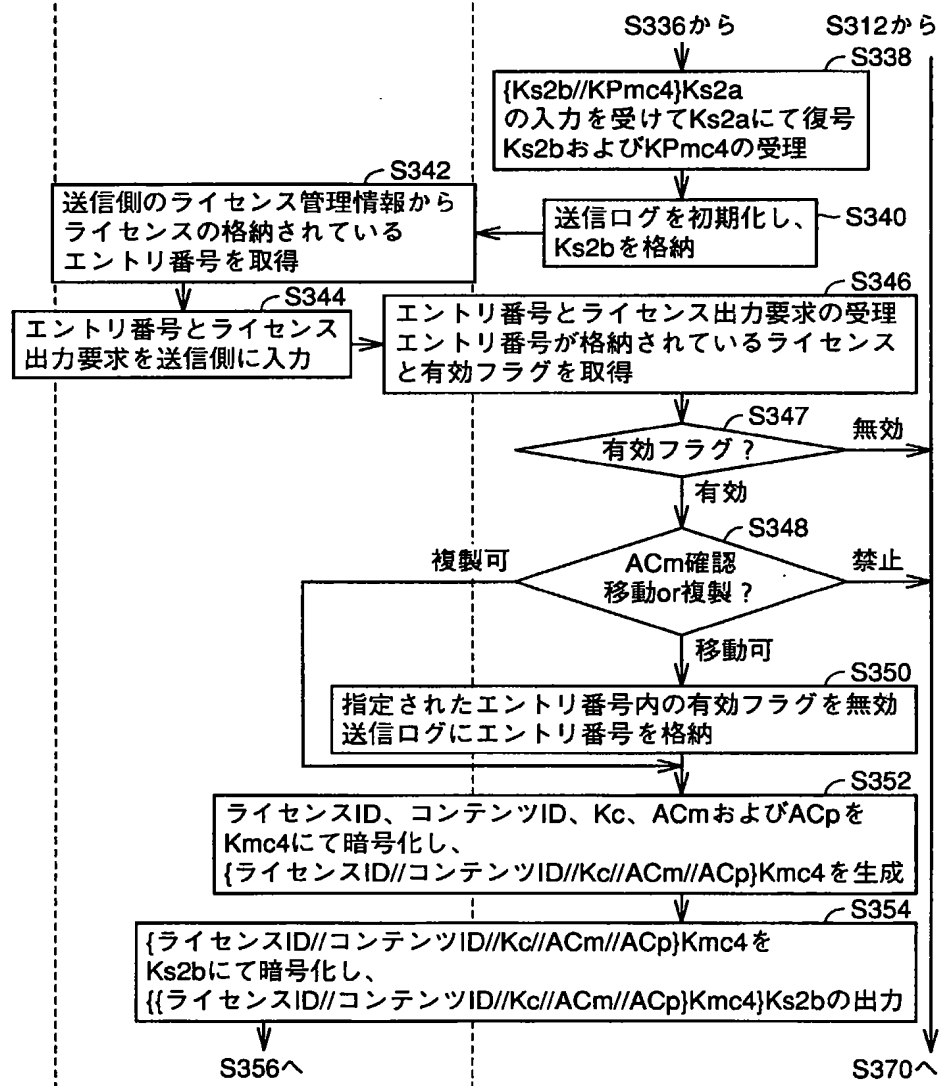


FIG. 16

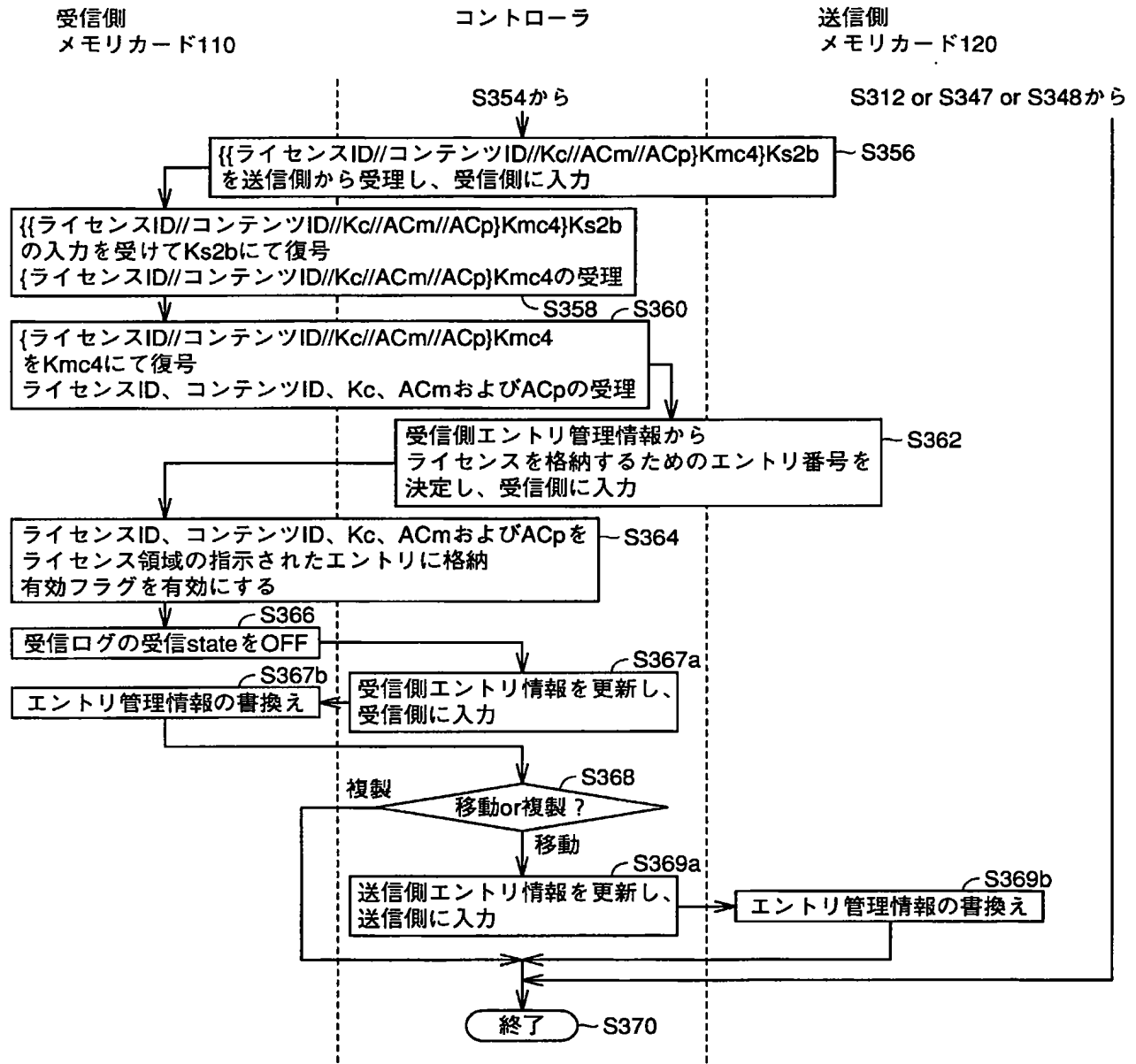


FIG. 17

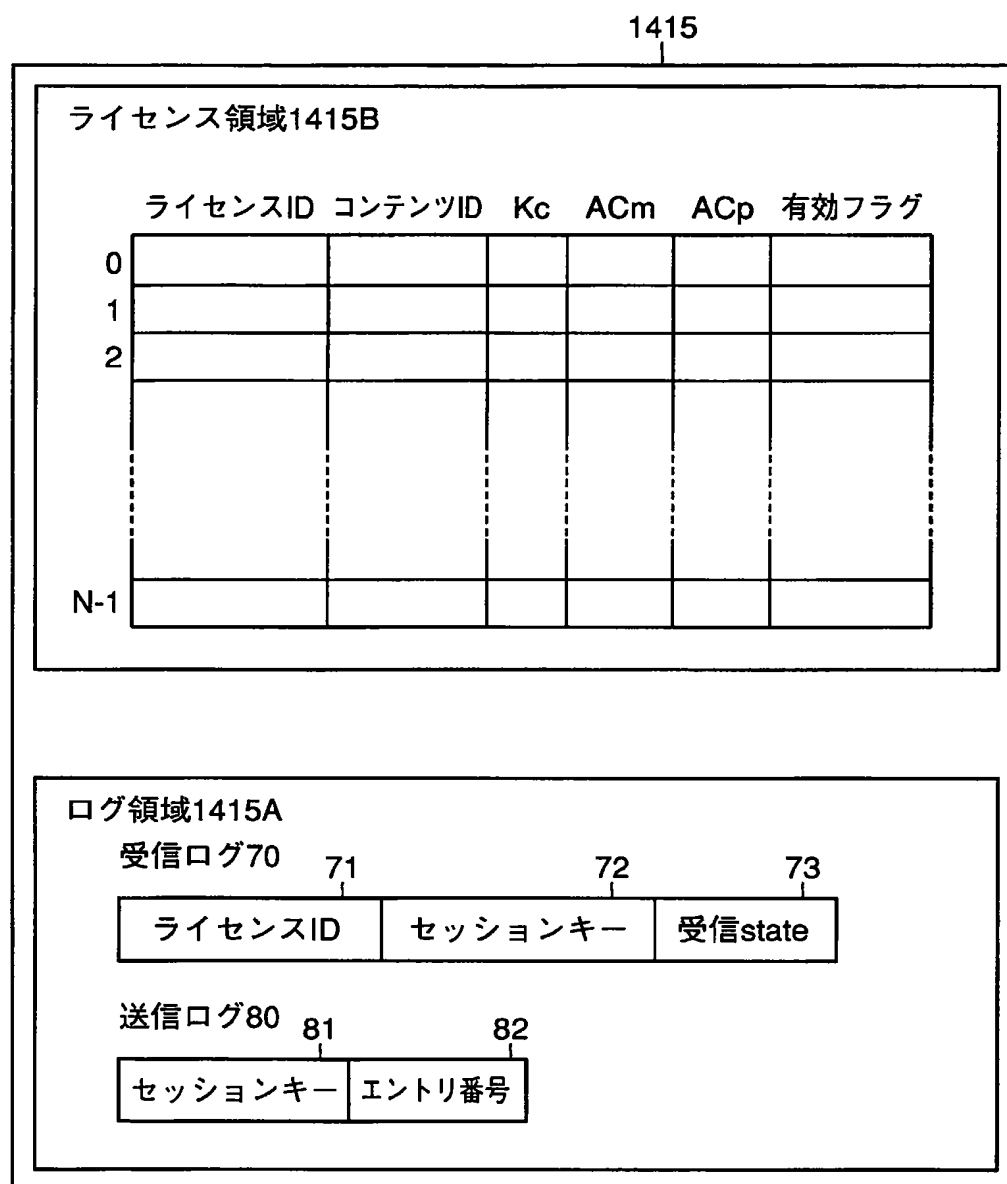


FIG. 18

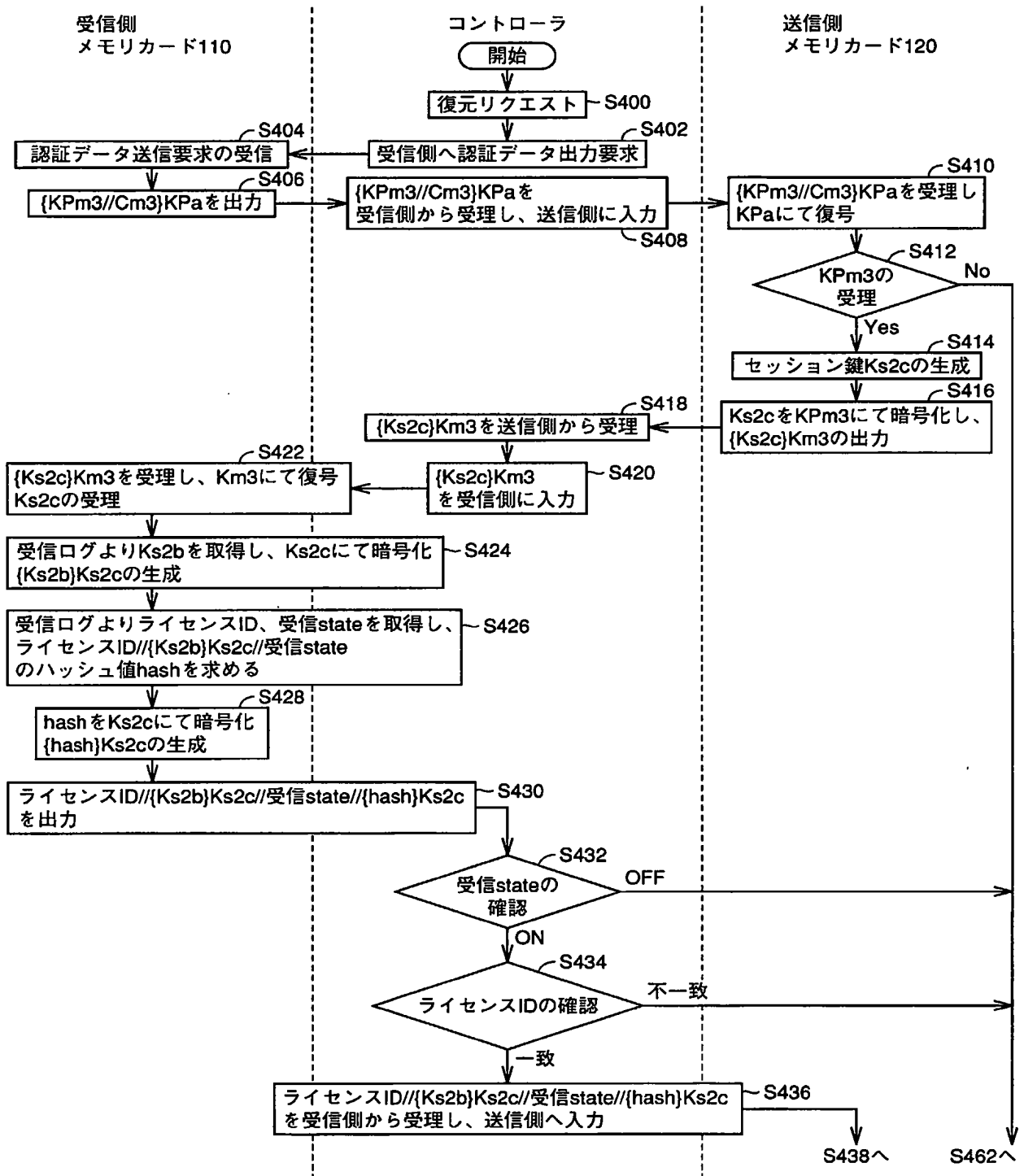


FIG. 19

受信側  
メモ리카ード110

コントローラ

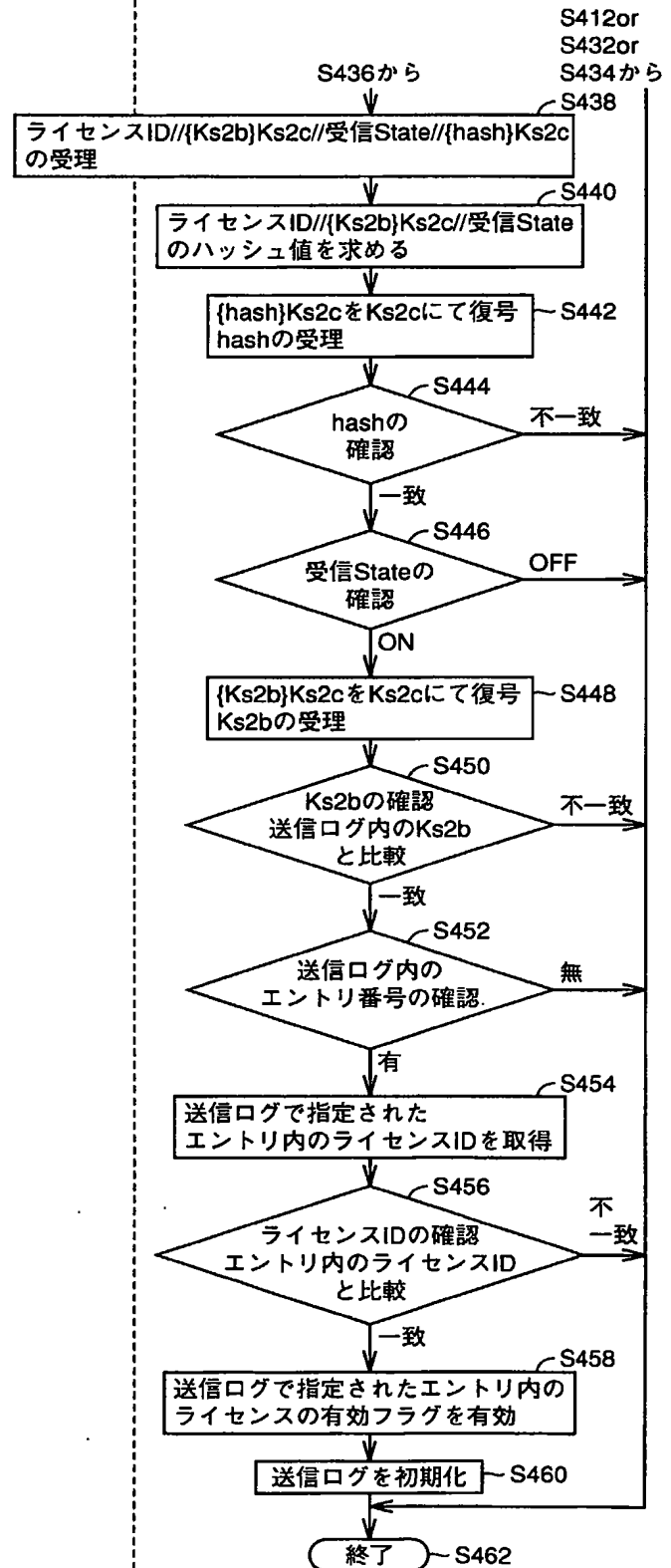
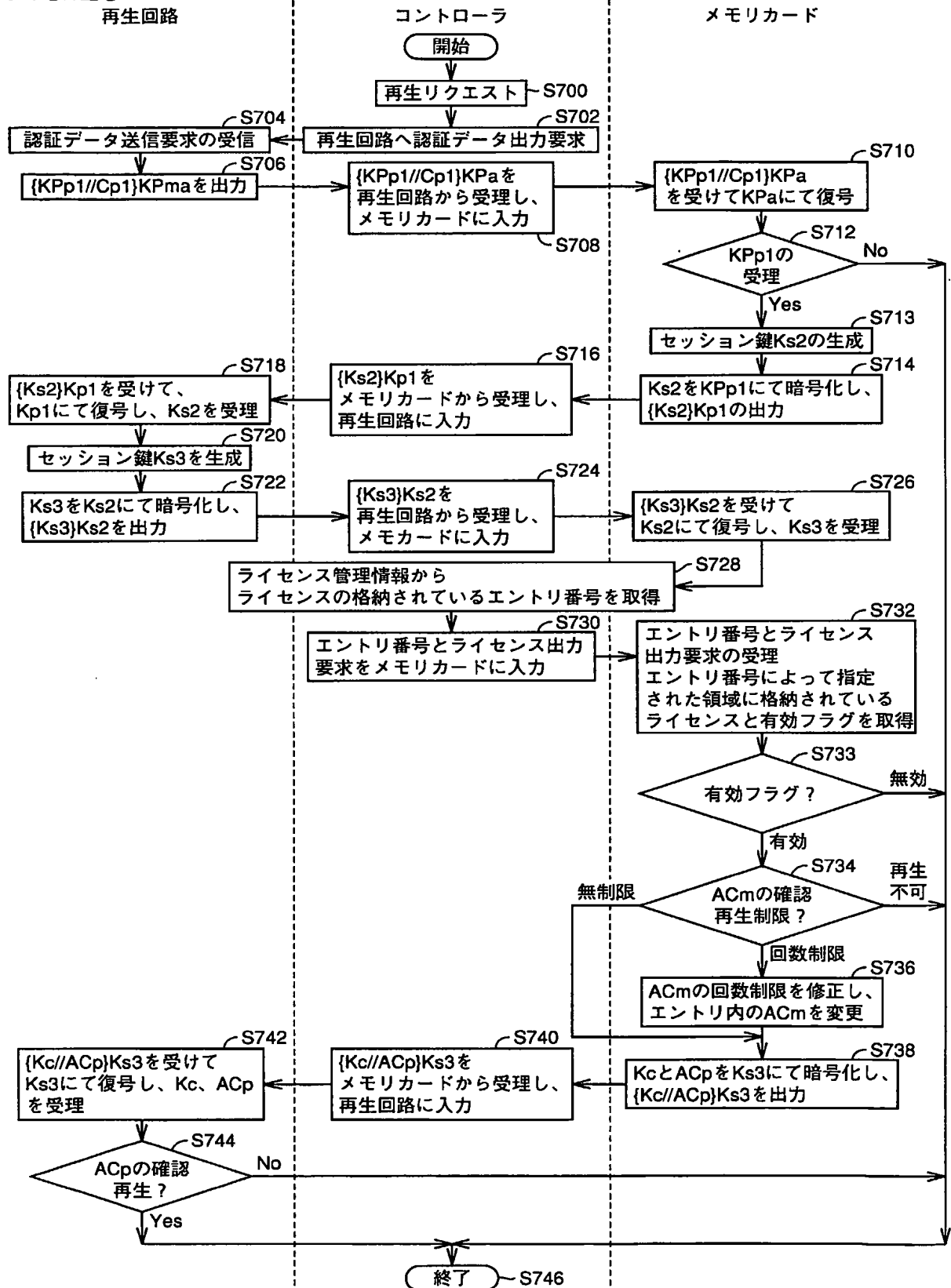
送信側  
メモ리카ード120

FIG.20





# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/07862

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F12/14, G06F15/00, G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F12/14, G06F15/00, G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Kokai Jitsuyo Shinan Koho 1971-2001  
Jitsuyo Shinan Toroku Koho 1996-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-305853 A (Victor Company of Japan, Limited), 02 November, 2000 (02.11.00), & EP 1047062 A2	1-16
A	JP 2000-285028 A (Minolta Co., Ltd.), 13 October, 2000 (13.10.00), Par. Nos. [0029] to [0034] (Family: none)	1-16
A	JP 2001-051906 A (Sony Corporation), 23 February, 2001 (23.02.01), (Family: none)	1-16
A	JP 2001-014221 A (Victor Company of Japan, Limited), 19 January, 2001 (19.01.01), (Family: none)	1-16
A	JP 2001-022859 A (Victor Company of Japan, Limited), 26 January, 2001 (26.01.01), (Family: none)	1-16

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
03 December, 2001 (03.12.01)

Date of mailing of the international search report  
11 December, 2001 (11.12.01)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F12/14, G06F15/00, G06F17/60

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F12/14, G06F15/00, G06F17/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996
日本国実用新案登録公報	1996-2001
日本国公開実用新案公報	1971-2001
日本国登録実用新案公報	1994-2001

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 2000-305853 A (日本ビクター株式会社) 2. 11月. 2000 (02. 11. 00), & EP 10470 62 A2	1-16
A	J P 2000-285028 A (ミノルタ株式会社) 13. 10月. 2000 (13. 10. 00), 段落29ないし段落34 (ファミリーなし)	1-16
A	J P 2001-051906 A (ソニー株式会社) 23. 2 月. 2001 (23. 02. 01), (ファミリーなし)	1-16
A	J P 2001-014221 A (日本ビクター株式会社) 1 9. 1月. 2001 (19. 01. 01), (ファミリーなし)	1-16

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

03. 12. 01

国際調査報告の発送日

11.12.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

梅村 勁 樹

5N

7313

電話番号 03-3581-1101 内線 3545

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2001-022859 A (日本ビクター株式会社) 2 6. 1月. 2001 (26. 01. 01), (ファミリーなし)	1-16